Marine Technologies' Control Networks Analysis and Optimization for Failsafe Operations Examined for Class Certification

By

Espen Løvø

Supervisors: Øyvin Simonsen, Matthias Pätzold, Tore Havsø

Project report for IKT590 in spring 2014

Faculty of Engineering and Science

University of Agder

Grimstad, 31 May, 2014

Status: Final 1.0

Keywords: Dual-redundancy, SNMP, Broadcast storm

Abstract

This thesis presents a suggested solution to improve Marine Technologies (MT) bridge systems. MT is advancing their technology and use Ethernet as a base. This is new in the offshore world and certification companies have yet to create clear lines to certify these network systems. Systems continue to get approved with their current protection, but measurements are needed to advance their protection and comply with new demands. The thesis will go through their current demands and interpret them to optimize MT's systems and give the certification companies a clear line to follow. The thesis will analyze MT's systems and experiment with solutions to optimize their system towards the certification demands. Through these experiments, a suggested solution is given through adding additional software in their systems to protect and monitor their network. In addition, the thesis is giving a suggested test procedure for the certification company to approve MT's systems.

Document History

Issue Number	Affected Chapters	Document history	Reason for change
0.1		First Draft	First Issue
0.2	All Chapters	Second Draft	Edit suggested by Supervisor
1.0	All Chapters	Third Draft	Final

Preface

Marine Technologies LLC provides this thesis assignment. As their current systems are still approved by certification companies, they need upgrades to comply with continuing new regulations. All of the work presented in this thesis is tested and analyzed at Marine Technologies office in Egersund. This thesis is not to be published and kept in secret due to the company competitive situation for a period of 2 years. Several individuals have contributed to this thesis. Tore Havsø, Stein Arve Aase, Thomas Kavle and Henrik Rasmussen from Marine Technologies. Ronny Olsen at Bristow Norway AS and Erik Jacobsen at Intelecom Group AS. Assistance Professor Øyvin Simonsen and Professor Matthias Uwe Pätzold from University of Agder.

Egersund

May 2014

Espen Løvø

Contents

1. Introduction:

MT produces bridge systems to the offshore industry. Their main products are ship control and navigation. Dynamic positioning systems (DP), integrated bridge systems (IBS) and thruster control systems (TCS). These systems controls the ship and/or share vital information from different sensors. All of these systems uses Ethernet network to connect nodes together for communication. These networks are dual-redundant to comply with certifications and standards given by certification companies. Each individual node needs certification for use offshore. The Ethernet communication between these nodes are new, and certification companies have not yet given clear lines of demands. Some measurements are made to protect the network against broadcast storm and looping. Filters and protocols used in managed switches gives these protections. Currently this goes through with Det Norske Veritas (DNV GL), but for how long. As their demands are not completely clear, discussions are ongoing on every system if it is fail-safe.

This thesis will go through the different systems produced by MT, evaluate them and give a solution on what changes is necessary to comply with new demands. The certification company DNV GL has given a list of demands they see as vital for approving. The task given for this thesis is to figure out what kind of errors can occur in these networks; how to protect, monitor, alert the system for any occurring errors. In addition to create a documentation, containing an argumentation that MT's network system is fail-safe to DNV standards.

1.1 Summary

The thesis goes through DNV GL's documents and interpret their demands towards a fail-safe network. Their demands is to monitor the network, protect it against worst-case scenarios such as a broadcast storm. Broadcast storms would flood the network and stall all other traffic, making it the worst-case scenario for a system relying on Ethernet network. MT's network is dual-redundant to comply with a safety net of a single point failure, but not a complete protection against broadcast storms. Current protection against this is a broadcast control within a managed switch. If the switch configuration is lost, no protection is given. Monitoring, alarming and protection against unknown factors are demands from DNV GL. Experimenting with a monitoring software, PRTG Network Monitoring, it is able to monitor, alarm and give commands towards any changes within the network. The experiments shows what nodes are vulnerable against a broadcast storm. Additional experimentation is given to shut down such a scenario. Through SNMP commands, a managed switch is able to shut down any port during a broadcast storm, excluding this node from the network. As MT has its own software development department, it is suggested they create a specified software towards this solution to provide a perfect protection against worst-case scenarios.

1.2 Problem Statement

The current network design used in MT's systems is based on Ethernet. This network is used in different systems like MT's IBS and TCS. In a TCS network, there are two Ethernet systems, main and backup. Each of these networks consists of a dual-redundant network. The backup system is segregated away from the main system to have two separate networks as a protection in case one of these networks shuts down. This network has a total of 4 networks shaped in a star configuration. Currently in this network there is a main switch which has a configuration that protects against flooding. This is done by having a limitation on broadcast on all ports and have a loop protection. This is not protection enough to get a certification for the network since there are no protection against other errors and no protection if that configuration is lost. These networks control the propulsion of ships, and it is vital that all of the systems are always functioning correctly and therefore certifications of all types of elements in their product are important. Currently DNV GL approves the networks, but with new demands and regulations arising, it will not last. With this as the main task for the master thesis, there are several other tasks that are included in the thesis:

- Find a solution on how a system alarm can be given if the network switch loses its configuration
- Find the best solution on how to monitor network load on the nodes connected to the network
- Find how these node(s) can be excluded, if the predefined max network load threshold is exceeded
- Create a documentation containing an argumentation that MT's network system is fail-safe to DNV standards
- Find, evaluate and analyze if autosense on speed, duplex and MDI can be used between all or static configuration regime needs to be implemented.

The main task for the thesis is to find an optimal solution for a fail-safe network with compliance of the certification demands. With this task, several of the tasks mentioned above will be included as the demands include monitoring, alarming and protecting the network. Secondary will be the documentation to argument for MT against DNV GL. If time allows, the thesis will look into autosense on speed, duplex and MDI.

1.3 Importance of the Topic

MT technology advances at a rapid rate. Focusing more of their communication towards Ethernet is new in their line of work. Most common is the use of serial data between nodes, making segregation a main focus and protection towards single-point failures. MT has been working in this business for many years, and continue to research and develop their technology to compete at the top of the world in this line of work. As their network communication do not segregate nodes, but create redundancy, it gives other challenges to uphold certifications. Their network has protection through dual-redundant networks and broadcast filter. Their newest advancement is changing leavers from serial data, to Ethernet. Adding more nodes towards a main source, the switch, enhances vulnerability. The switch contains configuration for these filters, but there are no protection for the switches if their configuration goes down. With their current systems on IBS and TCS, MT has continuing discussions with DNV GL considering the protection of the system if something goes wrong, such as a broadcast storm. Today, there are no precise certifications for a bridge network, and therefore DNV GL questions every system delivered by MT, towards broadcast storm issues. They do not see a broadcast filter on the switch as a sufficient way of protection. For MT it is important to create state-of-the-art products. By making a network fail-safe and approved by DNV GL, it would be the first bridge network with this type of certification.

Onboard vessels, protection towards crew and members onboard the ship is a vital and important factor. These bridge systems contains thruster control, Radar, maneuvering, autopilot, etc. Giving sufficient protection towards these systems are vital for survival if something goes terribly wrong.

1.4 Prior Research

Researching in this field is a difficult task. Offshore technology is not often publicized as technology competition is tough in this field. Therefore finding articles directly related is difficult. Creating fail-safe networks depends on the definition of fail-safe. Onshore a network can be fail-safe with only redundant nodes. The focus on prior research will be on papers found related to the task, and study MT's current network and what they have done with their network towards protection. As MT's systems are dual-redundant, this will be a first focus to understand and interpret what dual-redundancy means. Two articles towards network redundancy and protection related to the thesis is found and studied. With these two articles combined with the understanding and interpretation of MT's current network should suffice the background information to continue the research.

1.4.1 [1] Research paper 1: The implementation of a dual-redundant control system

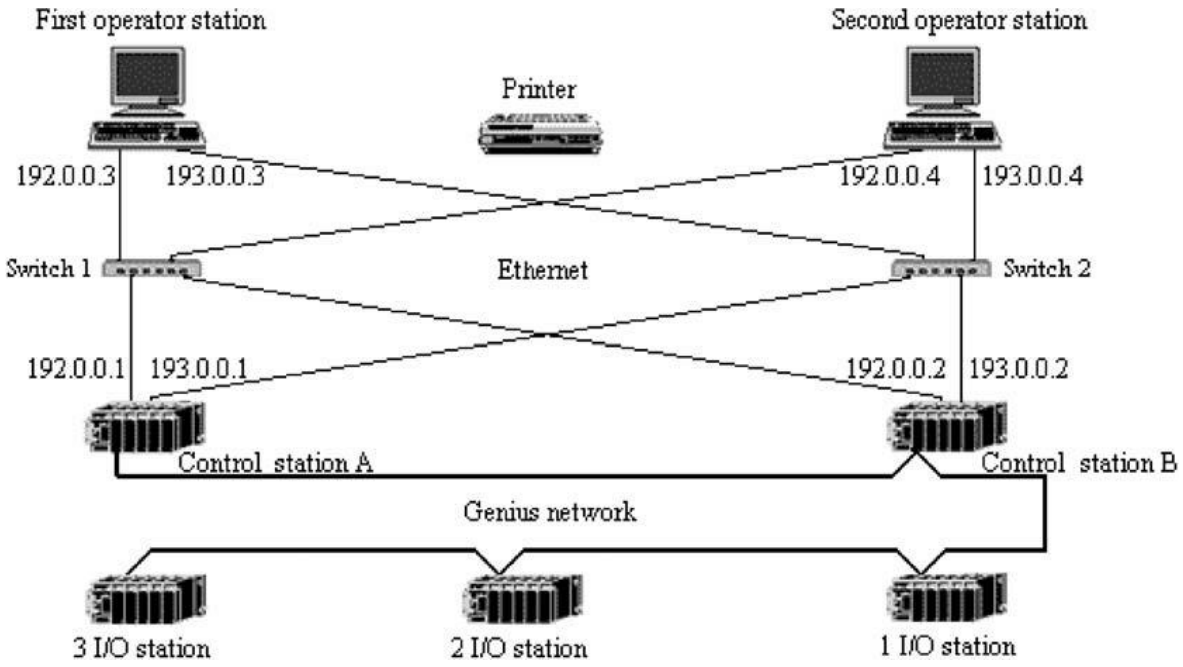


Figure 1: A dual-redundant network illustration

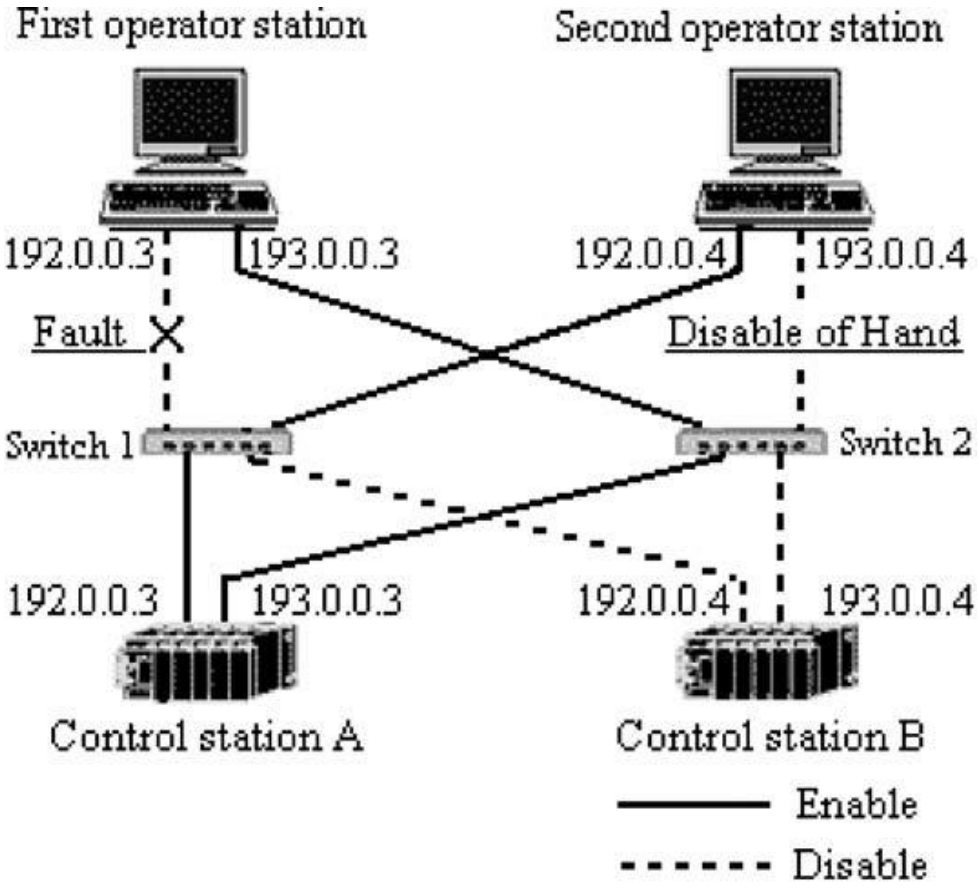


Figure 2: A dual-redundant network illustration with errors.

This research paper describes how to create a dual-redundant control system with Ethernet. They are using this system to control a continuous billet-bloom casting (CBBC) which is used in iron and steel factories. In this production, it is vital that the computer system does not go down during the production, and by using a dual-redundant control system on the operation stations, they have a safety net in case something goes wrong with either of the operating stations. What the paper states is that this redundant system can have several errors occurring without having the system go down. With figure 1 and figure 2 shown in this paper, it shows how a redundancy network might look like, and how it is still operational if an error occurs, respectively. This works by having each operator station and control station having two Ethernet adapters. By using two switches, one for an A net, and one for a B net, they have two individual networks connecting either operator station to either control station. With this

type of redundancy, three of any Ethernet cable can be disconnected, and the system will still be operational. In their network, they use TCP/IP protocol to be certain that the packages of information go through. They do not describe how TCP works, but explains how they use different IP subnets on the A and B network to divide them. There are two types of redundant network, active and passive redundant networks. The difference is that in an active redundant network, the computers share new information and updates their software. In a passive redundant network, there are no communication updates for the software.

1.4.2 [2] Research Paper 2: Resilience technologies in Ethernet

This paper covers about resilience technologies in Ethernet, which is the main technology used in network communication in today's networks all over the globe. Ethernet has improved the communication and replaced other types of technologies like ATM, private lines and Frame delay. With all the application requirements of Quality of Service (QoS), Ethernet has turned from no QoS in its early days to a full duplex gigabit network with Service Level Agreement (SLA). The SLA's highest priority is service availability compared to other parameters like jitter, packet loss and latency for choosing a service technology or service vendor. This means that there is a demand of minimum 99,99% service availability or higher. A network with this minimum service availability has for example a recovery time of 100 min and a failure rate of 10 occurrences per year. Since this is the main focus of SLA, the paper focuses on the resilience of the Ethernet across different types of protocols.

Redundancy is an important part in this paper, where redundancy helps against downtime and failure. Redundancy is explained well in the beginning of the paper and there are given examples of redundancy throughout so there is no question that the reader will understand what redundancy means in an Ethernet network. A redundant network can easily be described as a network where there is more than one road from source to destination. A package can complete its journey if an error occurs with either the medium or node along the path. There are some topologies that are automatically redundant compared to others. Ring and mesh has a built-in redundancy because of how it is created. In a partial or full mesh network some or all nodes are connected with each other respectively. A ring topology makes the nodes connect in a ring, making a loop where the packages can be sent in two different

directions and still get to its destination if one of the medium between the nodes is broken. The other topologies; linear and tree topology is without a redundancy without any extra technology since their topology does not make the packages give an optional path to its destination.

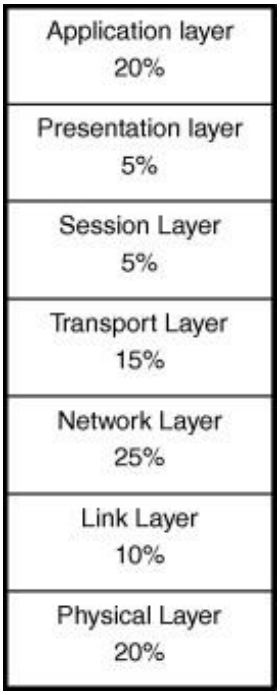


Figure 3: An OSI-model showing where the network errors occur in a LAN

Since network failures account for one third of IT related failures, it is important to put a lot of work into creating a network and making it as failsafe as possible. In figure 3, there is an illustration of where the fails occur in the OSI model. The network errors are distributed over the entire OSI-model.

A failure in the link layer might occur because of a damage cable or if an error occurs at the network interface. This is easily fixed if you have a redundant network where there is protocols that protects against these types of errors. In the physical layer there can either be a corrupt package that arrives at the receiver or as severe when a node fails and all the connection to this node is broken. Corrupted packages can occur either under transmission or propagation. This happens if one or more bits in the package is modified in the link. By using

an examining tool, the error correction checksum can be checked and the receiver can discard the package if it finds errors.

From what the paper states, there are different ways to protect your network, both on hardware and software. In the section of Protection mechanism they explains the difference protection levels between 1+1 protection and m:n protection. 1+1 guarantees 100% protection but is also the most expensive one. In a 1+1 protection level all the data sent through the network is replicated and sent through a different path in the network. When this package arrives to the destination, the receiver then drops the duplicate package. With m:n protection, the network uses a shared set of reserved resources where n is working resources that is protected by m protection resources. As recovery time is a main factor for service availability calculation it is an important factor to mention the cold and hot standby. The Hot standby which is one type of 1+1 protection means that both main and backup system starts up and traffic is sent simultaneously where the receiver drops the duplicated package. With this there are no downtime for the system to create a recovery time, but this consumes a lot of resources from the network. The Cold Standby is where the system has a backup that is predetermined but not in use. Whenever a failure occurs with the main system, the backup starts up and is used. This creates a recovery time before the backup has taken completely over.

A summary of the requirements and recommendations for each type of application.

Category	Services	Medium	Bandwidth	Delay/recovery	Jitter	Error
1	Interactive	Audio	4–13 kbit/s	<1 s (playback); <2 s (record)	<1 ms	<3% FER
		Data	NA	<4 s	NA	0
	Streaming	Audio	5–128 kbit/s	<10 s	<2 s	<1% pkt loss
		Video	20–384 kbit/s	<10 s	<2 s	<2% pkt loss
		Data	<384 kbit/s	<10 s	NA	0
2	Conversation voice	Audio	4–25 kbit/s	<150 ms	<1 ms	<3% FER
		Video	32–384 kbit/s	<150 ms	NA	<1% FER
		Data	NA	<250 ms	NA	0
	MEN	Bulk	NA	<50 ms, <200 ms, <2 s, <5 s	NA	0
3	Industrial Ethernet Network: PROFINET	Data	6.4–96 kbit/s	5–10 ms	<1 ms	0
		Data, Video	64 kbit/s–3.2 Mbit/s	150 μs–1 ms	1 μs	0
	Industrial Ethernet Network: SERCOS III	Data	96 kbit/s–2 Mbit/s	31.25 μs–1 ms	1 μs (hw), 50 μs (sw)	0

Table 1: "A summary of the requirements and recommendations for each type of application"

The paper continues with resilience requirements for different types of network and areas. Interactive media, end users Local Area Network (LAN), small businesses and

Metropolitan Area Network (MEN). Table 1 shows a summary of requirements and recommendations for different types of applications.

One of the important subjects in the paper is Industrial Ethernet networks. These types of networks have the most requirements of QoS considering the performance and real-time synchronization in many different industries. In many types of industry it is demanded for a minimum to none recovery time, considering the industry. If we take a flashback to article 1, where the network is sending information to control systems for production of steel and iron. If this network drops and have a recovery time of several seconds, disasters might strike in these factories.

Performance classes in an Industrial Ethernet Network are:

- Real-Time and deterministic behavior.
- High Availability
- Rugged and durable operation over extended periods of time

The typical grace time in an Industrial Network from IEC 62439.

Applications	Typical grace time
Enterprise management system	20 s
Automation management, for example, manufacturing, discrete automation	2 s
General automation, for example, process automation, power plants	200 ms
Time-critical automation, for example, synchronized drives	20 ms

Table 2: IEC requirements for grace time in different types of Industrial Networks

International Electrotechnical Commision (IEC) has created a table of requirements of grace time. Grace time is the recovery time and shown in Table 2. Many industrial companies has even harder requirements for their network than what IEC has set as a minimum.

Considering the high demand and requirements for the Industrial Ethernet Networks, there has been created new concepts of Real-Time Ethernet (RTE). Two of these that the paper mentions is SERCOS III and PROFINET.

Both of these protocols are meant to enhance the resilience and redundancy in the network. SERCOS III is only for line and ring topology networks while PROFINET can be covered in many other topologies. PROFINET is divided into different types; Component based Automation (Cba), Soft Real-Time (SRT) and Isochronous Real-Time (IRT). These three types have different approaches for redundancy and resilience, where all of these approaches uses Transmission Control Protocol (TCP).

Chapter 8 in the paper is the last chapter and covers many different protocols in different categories. There are 3 categories which is divided into the subjects: "End-user applications", "Interactive applications and MAN" and "Industrial Ethernet Networks". These are divided into these categories compared to their requirements for the network.

Category 1, End-user applications covers mainly about Spanning tree protocol (STP) and the variety of this protocol. STP is explained and illustrated quite nicely as shown in figure 4.

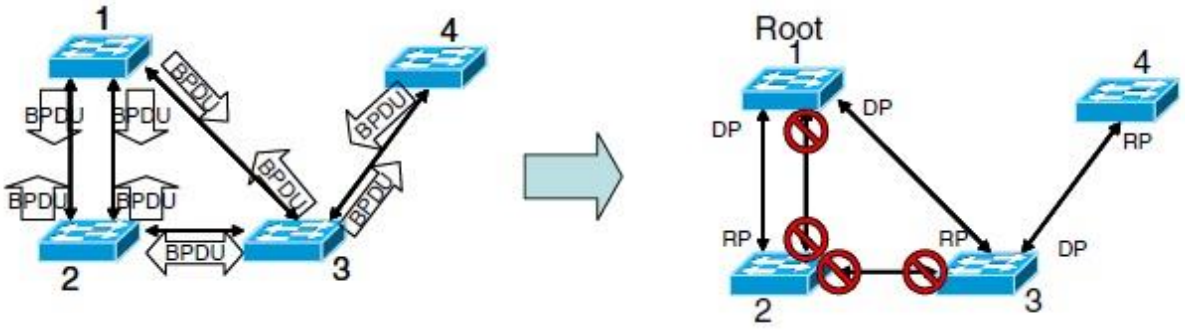


Figure 4: STP's process of selecting root node and block redundant links to create loop free topology

What the spanning tree does is protect against loop. In the illustration in figure 4 you can see it blocks the ports where it finds a loop to protect packages from being sent through the network as a loop, flooding the network. Even though packages have its time to live (TTL), packages are created so fast and flooded the network before the packages died out. Table 3 is taken from the paper to show the different STP protocols and their comparison.

Comparison charts for resilient protocols operating in end-user environment (continue).

Protocols	Centralized/ distributed	Backup path computation	Scalability	Standard/ industry	Synchronization
EAPS	Redundancy manager	Open blocked port	4096 VLANs, 64 EAPS domains	RFC 3619	Yes (complete flushing of FDB before restarting forwarding)
MRP (Foundry Networks Inc.)	Redundancy manager	Open blocked port	NA	Foundry Networks Inc.	Yes (complete flushing of FDB before restarting forwarding)
STP	Distributed	On the fly	Max 7 hop	IEEE 802.1	No
RSTP	Distributed	On the fly	Max 7 hop	IEEE 802.1w	No
MSTP	Distributed	On the fly	max 7 hop	IEEE 802.1s	No
ESRP	Redundancy manager	Switch to backup node	3000VLANs	Extreme Networks	Yes (master and slave nodes)
VSRP	Redundancy manager	Switch to backup node	NA	Foundry Networks Inc.	Yes (master and slave nodes)
VRRP	Redundancy manager	Switch to backup node	NA	RFC 3768	Yes (master and slave nodes)
RRSTP	Distributed	Open blocked port	Max 7 hop	Riverstone	No

Table 3: Showing the different Protocols in category 1

Throughout this chapter of category 1 protocols, there is illustration to almost all of these protocols to explain how they work and what they do. In general they are divided into which are used in what kind of topology. The VSRP and the VRRP are protocols to use when you are creating virtual networks within a physical network.

In category 2, Interactive applications and Metro Area Network (MAN), around half of the protocols cannot operate without interruption during a failure. All of these protocols mentioned in the paper are for mesh networks. An example of one of these protocols is *Smartbridge*. In this protocol it is important to know the topology in this network; frames with an unknown source are discarded automatically. This is a very good protocol for small networks where the administrator has very good knowledge of every node.

The last category, Industrial Ethernet Networks has very strict rules. As mentioned earlier, these type of networks have a high demand of QoS. Here they re-mention the classes of performance, Cba, SRT and IRT. In this category the predominant topology is ring topology, or double ring topology which is two rings where one node is connected in both rings.

Comparison charts for resilient protocols operating in Industrial Ethernet Networks (continue).

Protocols	Centralized or distributed	Topology	Backup path computation	Scalability/ nodes support	Standard/industry	Synchronization
MRP (IEC)	Redundant manager	Ring	Open blocked port on ring	50 (guaranteed performance)	IEC	Yes
HSR	Redundant manager	Ring, double rings	Open blocked port on ring	NA	Siemens and Hirschmann	Yes
HiPER-Ring	Redundant manager	Ring, double rings	Open blocked port on ring	NA		Yes
PRP	Distributed	Linear, star, ring	Overprovision by running a parallel network	NA	IEC	No
HASAR	Distributed	Single ring	Overprovision by sending a duplicate traffic	NA	IEC	No
DRP	Distributed/moving manager	Ring, double ring	Reverse dir on ring	50	IEC	Yes
CRP (at end node, not in switch)	Distributed	Doubly mesh	None	2047	IEC	No
BRP (at end node)	Centralized	Doubly connected to star, line, ring	None	~500+	IEC	No

Table 4: Different protocols in the category 3

One of the protocols in this category is Parallel Redundancy Protocol (PRP). This protocol uses two individual networks that run parallel to each other. Each of these networks can also have their own topology management protocol, meaning that you can have PRP on top and then RSTP or MRP underneath. As you can see from table 4 from the article, PRP can be used in linear, star and ring topologies. In this type of network the frames are sent simultaneously and the duplicate discarded at the receiver side.

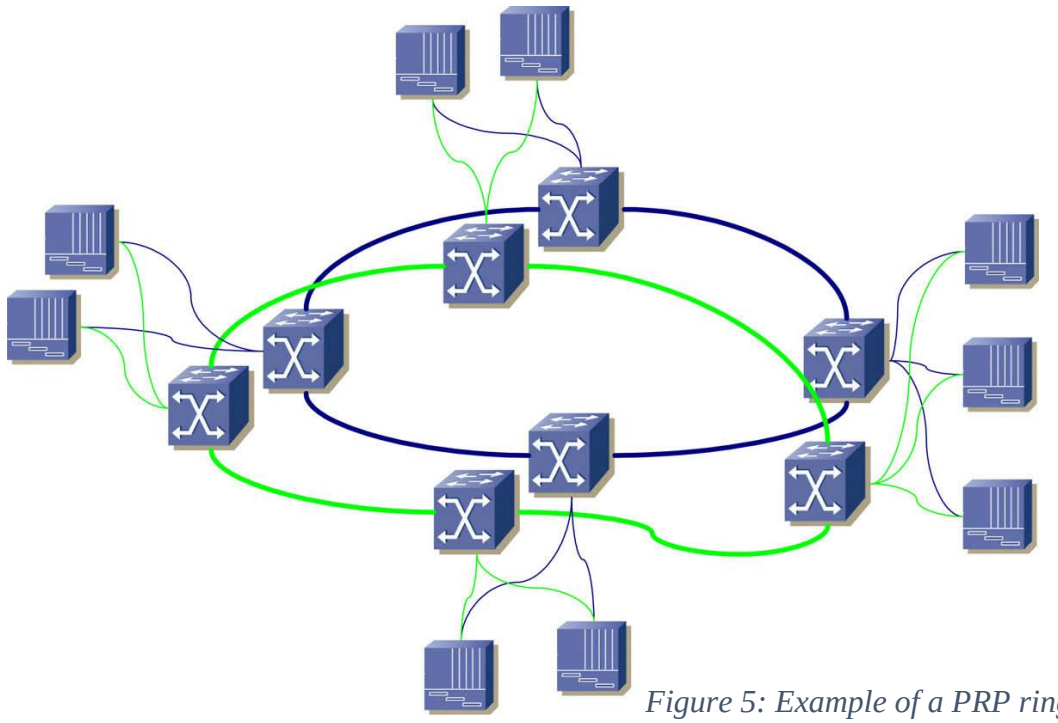


Figure 5: Example of a PRP ring topology

1.5 Experimental Research

Experimental research means that the thesis will experiment with the given topic. Instead of just reading and understanding the information, the thesis will do experimental work, and collect the data from these experiments to understand and to configure the network into the best solution for the given problem. A quote from Clarke, R.J to explain Experimental Research: "Researchers try to isolate and control every relevant condition which determines the events investigated, so as to observe the effects when the conditions are manipulated" [3].

The experiments that will be doing in this thesis would be recreating or using a network to the ones that is being used at MT. These networks are used in their products of DP, TCS and IBS. All of these systems are closed networks where all addresses are static. In some systems there is a single computer (VRAG) connected to the main system that can be used as a gateway for external assistance if the ship is out of reach from the project engineers. Since there is a physical separated switch connected either through a key or through a special command in the mode system, this network will be tested as a closed Local Area Network (LAN).

The experiments done in this thesis is setting up a network system and use a broadcast storm software on the system to see its behavior. Through these experiments, there will be a use of new software to monitor what is happening with the network, and do experiments on how to stop this broadcast storm as it arises. The thesis will do thorough investigation towards which monitoring software should be used and what solutions can stop a broadcast storm from happening. Data from the experiments will be collected and interpreted. This will give information if suggested solutions are sufficient towards a fail-safe network.

1.6 Methodology and research approach

The methodology that will be used in this thesis is quantitative research. Quantitative research is research that has a clear line of solution.

Firstly explaining the difference between quantitative research and qualitative research.

	Qualitative Research	**Quantitative Research**
Objective/purpose:	Objective is to gain understanding of reasons and motivations. To get insight in to an issue or a given problem. Can often be to generate hypotheses for Quantitative Research	Quantify the data, generalize it and sample it for a conclusive outcome.
Sample	Respondents selected to fulfill a certain amount of data. Normally a small number of non-representative cases.	Large amount of data collected usually with random selected respondents.
Data Collection	Collection of data is normally unstructured or semi-structured.	Structured collections.
Data Analysis	Non-statistical data.	Statistical data. The findings are conclusive.
Outcome	The findings cannot be used for a final outcome, meaning the outcome is not conclusive. It is Exploratory and/or investigative.	Used to recommend a final outcome

Table 5: Information about Qualitative and Quantitative Research [4]

The research that will be conducting is as mentioned with the intent of getting a sound solution to a given problem. By conducting tests of suggested solutions and observe what is happening, we can conclude from the results.

1.7 Offshore Safety

Creating any type of technology in the marine environment has different rules and standards than on land. The reason for this is the issue of safety. When offshore, there are no place to run or hide if an incident happens. For the safety of everyone onboard any vessel, it is vital that several systems have backup in case something goes wrong. For this reason, DNV GL has made strict regulations and standards for many different technologies that is used in the offshore environment. Several of these standards are used within MT systems. On a normal system, there are often a minimum of two of all types of sensors. This is to ensure the stability of the ship, but also to fulfill the rules and regulations of DNV GL, depending on the system. It is also important to notice not just any sensor can be used offshore. This equipment needs to be certified by DNV GL or other certified companies to be certain the equipment can withstand the harsh environment of the sea. Every node in MT network system has been tested, and certified by DNV GL regulations.

The requirements for this thesis is under the chapter: 3. DNV GL demands and regulations.

1.8 Report Layout

1. Introduction.

Introduction covers the description of the task ahead and the importance of the task. It also includes prior research and the thesis research approach.

2. Marine Technologies and their systems.

The chapter contains MT's most common components and what different systems they produce, such as Dynamic Position, Integrated Bridge System, Thruster Control System and Backup System. It also contains MT's dual-redundancy example and the systems connection to internet.

3. DNV GL demands and regulations

DNV GL's documented demands for a ship network.

4. Demands analyzed and interpreted

Goes through DNV GL's demands and compares them with MT's current systems.

5. Suggested Solutions

Gives different solutions to cover all demands by DNV GL, through self-protective nodes, adding more nodes, self-sufficient switches, adding anti-virus on a permanent basis and an evaluation of all solutions created.

6. Solution

Describes the best solution through combining different solutions from chapter 5. This chapter is divided into two sub-chapters. 6.1 covers the solution and testing of technology needed for this solution. 6.2 covers additional suggested improvements to enhance their network.

7. Conclusion

8. References

9. Appendix

2. Marine Technologies and their systems

2.1 Components and Current systems:

The network in the different products varies from system to system. Since rarely any ship-build is identical, they often want different equipment and different types of systems in their ship. Since this is a big factor, there are different types of networks at play. In general, any of the networks is a star topology network, depending on the amount of switches needed. There are mainly three different types of networks. Within these networks, there are several types of components.

- **Operator Computer (OC)**
  The "OC" is an operating computer, where all the information is shared with the user. On this computer, the user can get information or give commands to the ship while in DP mode. When these computers are connected with a screen, they are called Operation System or "OS" in the software.

- **Control Computer (CC)**
  CC is the control computer, and a vital part of the system. This computer is the middle man between the OC and the IO cards. This computer collects and sends the vital control functions from the OC and the IO cards.
  Normally in a system, there are three of these computers. The reason for this is to use MT's voting algorithm. The principle of this algorithm is a voting process where two out of three wins and the one that disagrees is voted out. If CC3 is in command, and the two collects different information than the CC3, then the CC3 is voted out and one of the others takes command. This is done to be certain that the information sent to the IO cards and the OC is correct.

- **Interface Unit (IO)**

  IO cards are the connection between the network and different elements. These cards convert serial data and packet data, and send them to their respectively receiver's. This card is multifunctional and used for several types of operations. Thruster's IO cards, Power IO cards or as a Panel IO cards. In some systems, these cards are swapped out with computers (gateways) to do the same job. This is usually done in a TCS. The IO cards are programmed by Field-programmable gate array (FPTS).

- **Operator Panel (OP)**

  The operator panel is the panel where you can take control of the DP system and do various commands. It contains several buttons for these commands and a joystick for manual steering. Often in DP systems, this operator panel's IO card includes where the serial data from sensors are picked up and transmitted to the network.

- **IOB Leaver Card**

  These small cards are in principle a small version of the IO card. It translates serial data, convert it into data packets, and sends it through the network. Software on these cards are lightweight IP (lwIP).

- **Mode selector unit**

  This unit is the selector for what kind of mode you want the system to be in. In addition, the unit switches the system between main and backup systems. The unit is connected to a Mode Panel by independent cables. This panel is where the operator chooses between different modes such as autopilot, DP and backup.

- **Compact OS**

  This computer is a special independent computer. This computer has its own touch screen with either a joystick or heading wheel connected. This computer also uses 24volt (V) connection and is often used as a backup computer since it has both the DP system and a manual joystick in one node.

- **Switch**

  The switch varies depending on the system. It is the connection between all of the nodes, and in smaller systems, it is a “dumb” switch, which states it is not manageable. This node itself is the core of the network. Every other node is connected to a switch, depending on the size of the system, it has one or more switches for either networks. The switches are set up in a star topology, meaning one main switch as a center. In the managed switches, they use RSTP protocol and broadcast storm control filter for protection.

The network itself is divided into either two networks, Network A and Network B, or in 4 networks; Main network A and B, backup network A and B. the latter is used in thruster control systems. The system is similar to PRP although they do not use the protocol. It is also a cold standby network, where network A is their main transport of packages. If network A does not respond, network B will take over after a grace time of 1.6 seconds. Which is within the limits of automation management requirements for industrial networks. Their system has in addition a buffer time for the A network to get back online and be stable, before the system decides to switch back to network A. It is a dual redundant network, using spanning tree protocol for protection and broadcast storm control for protecting against broadcasts.

2.1.1 Dynamic Position (DP)

DP means that the system control the ship to maneuver depending on what maneuvers you want. A DP system can:

- **Hold a precise position on longitude and latitude.**
- **Hold a precise position depending on a ship or platform**
- **Hold a precise heading as another ship. (using the other ship as a reference)**
- **Be able to move a ship x meter in any direction or rotate any angle.**

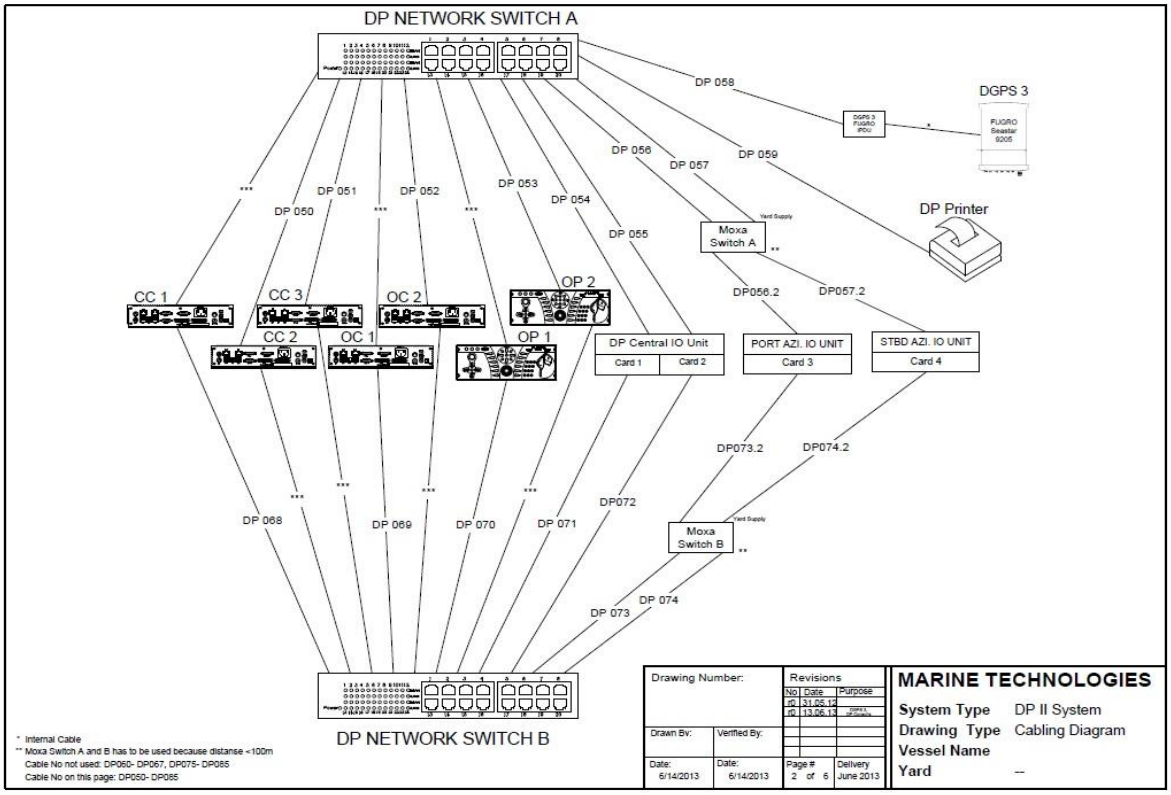


Figure 6: An example of the network in a DP2 System

DP is the main system where there are simple layer 2 switches with no configuration or managed switches, depending on how big the DP system is. In these systems, there are information sent through these switches between several types of nodes.

In figure 6, there is an illustration of a DP 2 system. A DP 2 means that there is a dual-redundant network in the DP system. As seen in the illustration, every important part of the system connects to two separate switches. In addition, there are two OC's, three CC's, and two OP's to comply with redundancy on every level. The IO units are the control cards for the thrusters. In this illustration, the port and starboard azimuth thruster are divided into separate units. If one of the IO cards fails, it does not mean that both thrusters will fail. The same with the DP central IO Unit, it states that this unit has two separate cards for its usage, this is often for two bow thrusters, one card for each thruster. With a system like this, you can lose much of the equipment and still be able to control the ship.

2.1.2 Integrated Bridge System (IBS)

Integrated Bridge System (IBS) is a bundle of different components into one system. An IBS often contain systems like:

- Radio detection and ranging (Radar)
- Electronic Chart Display and Information System (ECDIS)
- Horisontal Connection System (HCS)
- Automatic pilot (Autopilot)
- Helideck Monitoring System (ShoreConnection)
- Radascan (DP Sensor reference view)

As the DP is controlling the ship while doing its operations, the IBS is a segregated system from the DP. Before there was one station for each type of system, with the IBS, all these systems are integrated, and the information can be shared and available on any IBS station. On the IBS station you can access all the information you have on the DP and additional information as Radar, chart computers, thruster information and ballistic information. Usually there are an autopilot in the IBS system, but there can also be a backup system for the DP in the IBS.

In some occasions the customer wants a backup system if all else fails, or to have a mobile system that can be used several places throughout the ship. To get this system certified as a backup, it is segregated from the DP system. In some occasions, the backup system gets integrated into the IBS, since the IBS is also segregated from the DP system. This backup system is often a Compact OS, which is connected through a special Network cable that includes both network and power.

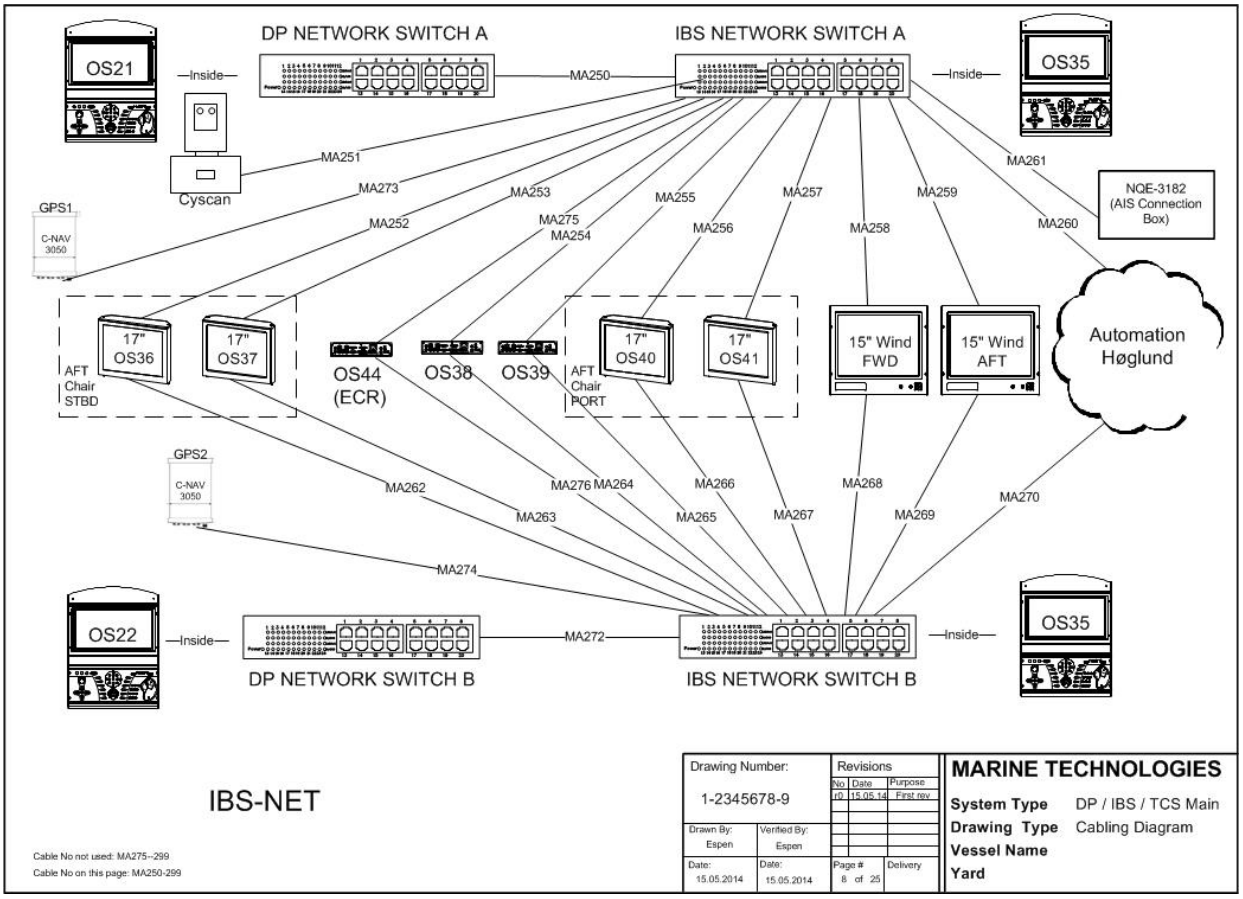


Figure 7: This figure illustrates parts of a network within an integrated bridge system

In figure 7, you can see that the complexity has increased compared to a DP system. There are a lot more computers connected, and in this illustration, you can see that the switches are referring to a second switch. This system is dual-redundant as well as the DP system to protect the system in case some element goes down.

2.1.3 Thruster control system

A Thruster Control system is a system where MT also have control over the thrusters through leavers. In these systems additional to all the DP system, there are thruster handles and special CC that is connected to the system. Since redundancy is an important factor, a double handled thruster handle gets up to eight output network cables connected to this handle. These handles sends out serial information and is connected to the IOB leaver cards. To use this handle as an example of connection, a double handled thruster is used to handle

two tunnel thrusters, one for bow and one for aft. Since these tunnel thrusters package traffic should be dual-redundant and segregated, there are a main net A/B and a backup net A/B cable for each bow thruster out from this handle (4 cables for each thruster). To make sure that this handle can be used for both main and backup system, it also includes a net A and net B for backup. In total this will make this handle alone have 8 network connections to different parts of the network. Considering there are more than just 2 tunnel thrusters on the ship, and usually there are several spots where the officers wants to steer the ship, the amount of cables and connections are increased rapidly.

2.1.4 Backup system

Often a system has additional backup to the dual-redundant system if everything else fails. This system is completely segregated from the DP system, have its own IO card connected to the thrusters, and has its own sensors. The only connection the backup has to the rest of the system is a serial connection to the mode selector unit. Depending on the size of the backup network, it can contain as little as one sensor, one CC, one Compact OS, one IO card and one switch to connect these.

2.2 Dual-redundant network and remote access

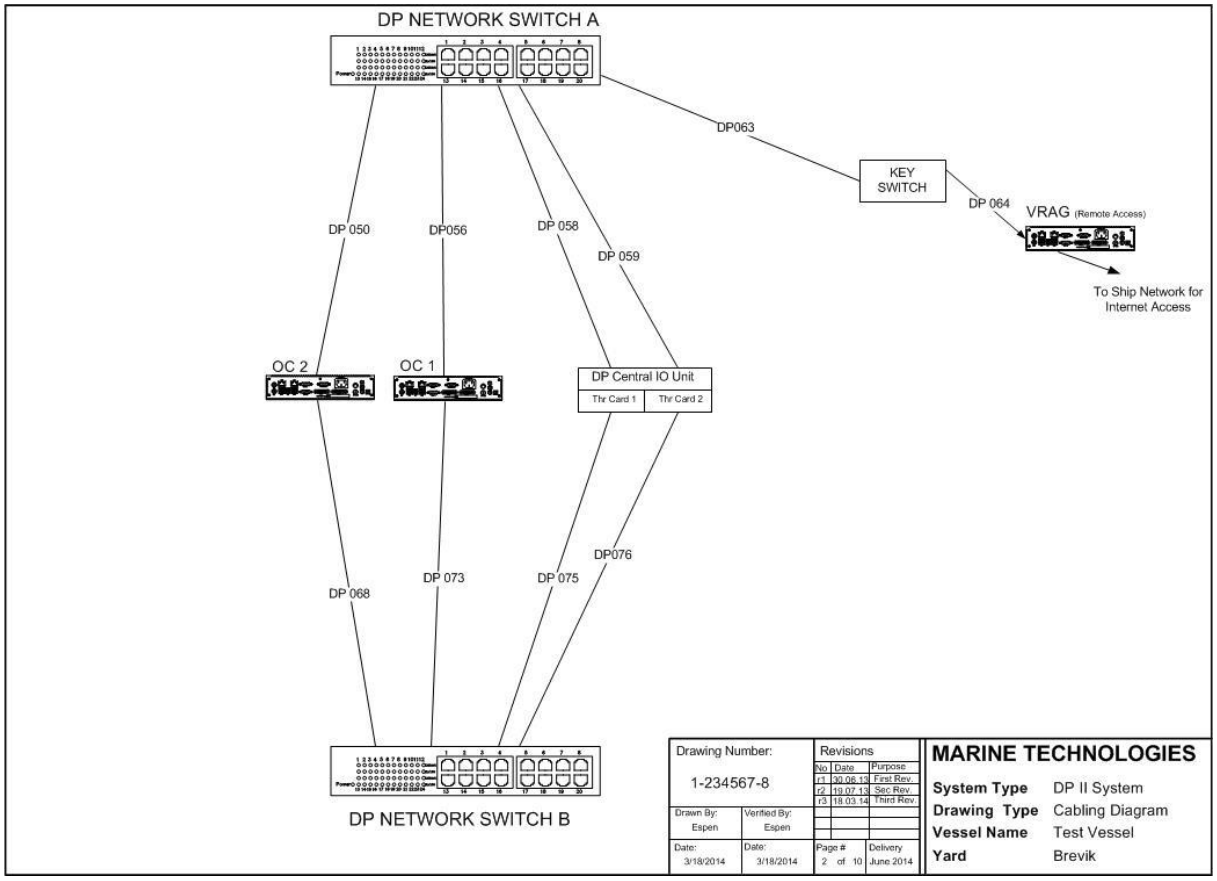


Figure 8: An example of a dual-redundant network

Redundancy means that there is an overabundant of an element. In network terms, it means there are more than one road to its destination. As mentioned in the research paper 1, a dual-redundant network, you have two segregated networks towards your destination. Figure 8 is an illustration of a dual redundant network in a DP system. there are two paths for each operator station to reach each of the control stations respectively, making it 4 roads for each operator station to control the system or part of the system. There are two operator computers and a DP Central IO Unit with two IO cards. Each IO card can be able to control two thrusters. If we divide two main thrusters and two tunnel thrusters, we would have one of each on each IO card. While doing this there is a possibility to still drive and maneuver the ship with one IO card out.

In addition, this figure includes a Vessel Remote Access Gateway (VRAG) computer. These computers are the connection to internet if there is any need for remote control of the system. Often in small cases, small updates or adjustments, the project engineers at MT can connect to the ship through the VRAG. The important thing here is that the VRAG does not always have a clear connection to the system. In the illustration, you can see there is a "KEY SWITCH" box between the system and the VRAG. This is either a physical key, or a mechanism inside the mode selector, which the captain has to turn on for the VRAG to have access to the system. With this type of switch, the system is physically detached from the outside world when turned off.

2.3 Current network technology

2.3.1 Patch cables

In this type of industrial systems, it is important to choose the right type of Ethernet cable. The chosen cable for these systems is a Category 6 cable (CAT 6). What this means is that the cable is meant for speeds up to 1 Gbit/s. The chosen cable is also a Plenum rated cable. Normally the patch cables are created with PVC, which creates a toxic smoke in touch of fire. Considering safety as the highest priority, the plenum rated cables do not create a toxic smoke in touch of fire. The CAT 6 cables, which are in use in the system, are the cables that the company provides internally in the system. All other cables where the shipyard is providing, MT demands a CAT 7 cable, but can be terminated as CAT 6 [5].

2.3.2 IPv4

The system operates on Internet protocol version 4 (IPv4). IPv4 is still the main operative protocol in the IP world although Internet Protocol Version 6 is growing in all of the world's corners. There is no need for this system to change into IPv6 today, considering this is a closed LAN, where issues for not enough IP addresses will never be a problem considering the total amount of nodes in this system is nowhere near the 4.3 million addresses that the IPv4 can achieve. Considering the other traits of IPv6 in this system is another thing. The new type of IP might have traits that can give improvements for this system, but not prioritized at this time [6].

In MT systems they use static IPv4 addresses, and have different IP tables for each type of node. Such as CC uses range 11-19 (192.168.0.11-19) and Switches uses range 240-249. IOB leaver cards and IO cards uses special address wheels called Most significant bit (MBS) and Least significant bit (LSB) to set their static IP addresses [7]. IO cards use 170-179 and the IOB leaver cards use 180-199.

2.3.3 Protocols: TCP/UDP

Most of the traffic used in this network is UDP traffic. UDP is a typical protocol for live feed information that is needed for quick response where quick updates are more important than safe updates. UDP is often used in multimedia streaming across the internet. If you lose a pixel or a few microseconds of a voice call in a lost package, it does not interrupt the total value of the information. In UDP the packages are sent fast and with a minimum of service. In our system it is more important to get updated information from a thruster handle on how much force the thruster should give. In TCP, which is the most normal traffic protocol on the internet, there is a check whether or not the packages have arrived or not. This is good for e-mails and other important information where it is more vital to have the correct information. With video streaming or in this case, thruster information sent; it is more important that the information is sent quickly and often, than use time to check if the information is correct and cause delay [8].

2.3.4 Spanning Tree Protocol

The Spanning Tree Protocol (STP) is an old protocol that is in use in almost any managed switches today. Either its original state as an STP, the 802.1D version, or other types of this protocol. STP mains focus is to avoid looping of packages within a network. When several switches is set up in a network, as a ring topology, the STP shuts down one of the ports in this ring topology, to avoid that packages will go in a loop through all the switches if a package cannot reach its destination. STP does not close this port permanently, considering another switch might go down, it will then open its port to still have access to the entire network.

All packages have a Time To Live (TTL) time which theoretically is calculated in seconds. The normal way to calculate TTL is in hops, meaning how many routers the package needs to go through to reach its destination. This is why in IPv6 TTL is renamed into Hops.

Rapid Spanning Tree Protocol (RSTP) is a further development of the STP. Since the STP can use up to 30-50 seconds to respond to a topology change, the RSTP only needs a few seconds or even milliseconds if it is a physical link failure. RSTP is the currently used STP type [2].

2.3.5 Unicast, multicast, broadcast.

A node can send packets either to one node, several nodes or all nodes. These types are unicast, multicast and broadcast, respectively. How a package is decided to be a unicast, multicast, or broadcast, is decided by the software and that information is stored in the IP header.

Unicast is when a node sends out information to just a certain node and decides this is the only node that needs this information. This is good if the packets you are sending out should only reach one node. When the switch receives this information, it notices that the package is a unicast, and will forward the package only to the port where the receiving node is placed. Consider if you want to send out the same information to several nodes, this can be done by unicast, but the source node will have to send the same package as many times as the number of nodes which needs this information.

A multicast on the other hand is a package that will be shared to several nodes and is used with several nodes needs the same package from one node. The source node sends out one package, and the switch will in this case have a list of subscribers to multicasts and will send this package to all the subscribers to this particular package. This makes multicast more efficient than unicast if you are sharing the same information with several nodes.

Broadcast is sent from the receiver to the switch, and the switch will send this information on all ports. The biggest problem with the broadcast is the risk of flooding the network considering messages from a broadcast are usually necessary to be interpreted by every node [9].

2.3.6 MT software and network traffic

Their computer and nodes contain different types of software to communicate and handle the different data. Their main DP system is control by Marine Technologies Operative System (MTOS). On bigger systems like IBS and TCS, they use an application manager as a base, and add MTOS and different software such as Thruster Control System Software (TCS), ECDIS, Conning etc. MT has focused their programming on UDP traffic as most of the systems operational functions demands live feeds. There are used both unicast and multicast messages through the network, depending on the customers desires. The SSB and Radar in some cases uses multicast.

The traffic is set up to protect in a special manner,

This coding checks if the message is a broadcast message, and will throw away the package if it is a broadcast message. These cards communicate on a different level than a normal computer. They use designated ports to communicate with different CC's. MT has designed their communication in a special way. When communicating with the CC's, the packets are sent through designated port numbers for each designated node.

2.3.7 Alarms

The system already contains a significant amount of alarms towards their system. Focusing on the network side of the alarms, an alarm will immediately set off if a node does not respond to any request made by any node. There are no alarms going off incase Control Processing Unit (CPU) load or hard drive load is close to maximum.

2.3.8 Switches

There are three types of switches used, depending on the complexity of the system and where the switch is implemented. There are two unmanaged switches and one managed switch. The SMC unmanaged switch is used in standalone DP systems. The other unmanaged switch, Sixnet unmanaged switch is a 24Volts (V) switch used in the small backup systems.

This switch is used here specifically to remove 230V from the entire backup system and make it run only on 24V. The last switch is a managed Netgear witch. A managed switch is able to do configurations to the network through its management and handling of data packages. The Netgear switch is used in IBS and TCS. This switch is set with a static IP address, with additional RSTP and a broadcast storm control to protect the network.

Figure 9: Netgear GS728TP Managed Switch

3. DNV GL demands and regulations

The IEC is a commission that creates international standards for all types of electrical and electronic devices. All these devices go under a term called “electrotechnology”. The IEC is a non-profitable and non-governmental organization. There are 82 members, or countries in the IEC. The rules and regulations DNV GL follows, are standards usually provided and created by IEC [10].

DNV GL is a newly merging company between Norwegian DNV and Germany GL. They are one of the largest certification companies in the world, and are recognized for their knowledge and consultations towards the marine industry. They have given a list of demands towards their interpretation of what is necessary to have a failsafe network.

What determines that a network is failsafe depends on the interpretation. Making a failsafe network could be as simple as making it a dual-redundant network. For the certification company, this is not enough to make the network reliable and failsafe towards their interpretation of a failsafe network in the marine industry. They have made a list of demands that they have interpreted and wants to be fulfilled for approve a network for failsafe.

Their demands are collected out from their document “Nautical Safety” [11]

“D. Network based integration of navigation systems (ICS)

D 100 Independency and Integrity

- **101:** The network integrating the ICS shall be designed with adequate redundancy of independency.

- **102:** Cables and network components belonging to redundant networks shall be physically separated; by separate cable routing and installation of network components belonging to the redundant network in separate cabinets, power supply to such units included.

- **103:** Each network shall function independently and it shall be possible to protect each network from unnecessary traffic on the other network.

- **104:** All network components controlling the network traffic and nodes communicating over the network shall be designed with inherent properties to prevent network overload at any time. Neither the nodes nor the network components shall be able to generate excessive network traffic or consume extra resources that may degrade the network performance.
    - **Guidance note**: The nodes and network components shall have properties to monitor its own communication through the network, and to be able to detect, alarm and respond in a predefined manner in case of an excessive traffic event.

- **105:** The performance of the network shall be continuously monitored, and alarms shall be generated if malfunctions or reduced/degraded capacity occurs.

- **106:** Any powered network component controlling the network traffic shall automatically resume to normal Operation upon restoration of power after a power failure.

- **107:** All nodes in the network shall be synchronized to attain a uniform time tagging of alarms (and events) to enable a proper sequential logging.

- **108:** The network shall be designed to withstand exposure to electromagnetic interference
    - **Guidance note:** The wheelhouse is exposed to high voltage equipment and RF transmitters. Reference is made to Classification Note No. 45.1 for guidance on EMC measures.

- **109:** Any Closed Circuit Television (CCTV) system shall not be part of the ICS network.

E. Malfunctions and restoration

E 100 Failure effects

- **101:** A failure of one part shall not affect the functionality of other parts except for those processes and functions directly dependent upon the information from the defective part.
    - Any one part or node can be shut down, and this will not affect any functionality of the rest of the system. If a broadcast storm arrives in network A, this network is still segregated from network B, and network B can be used to control the system.

- **102:** The ICS response to malfunctions shall result in the safest of any other configuration or mode of operation.

- **103** *Fall-back arrangement:*
    - One of the servers including at least one multi-function display (MFD) shall continue to be available as a stand-alone ARPA following failure of both networks.
    - One of the servers including at least one MFD shall continue to be available as a stand-alone ECDIS following failure of both networks.
        - **Guidance note**: An exception from this general principle may only be approved for completely independent networks based on documented design features and analysis that is verifying that any logical failure, including uncontrolled broadcast of data packets (network storm), of any computer connected to the networks cannot cause loss of/failure of more than one of the networks.

F. Testing

F 100 Network test and verification

- **101:** The network functionality shall be verified in a test where at least the following items shall be verified:
    - The main observations from the FMEA
    - Self-diagnostics
    - Worst-case scenarios – network storm
    - Network segregation – autonomous operation of network
    - Individual controller node integrity – workstations working without network communication.

“

With these particular rules and conditions it will determine a suggested solution. This solution will be able to prove the design will protect the system from errors.

4. Demands analyzed and interpreted

Looking over the system, there are several improvements that can be made, but there needs to be the focus to apply with the demands from DNV GL to make it certified. The system has several of the demands in place already, and it is needed to check what they cover and give a suggestion to comply with all demands.

By going through the list step by step, we can analyze what they have done and how it complies with the demands.

D 100: Independency and Integrity

101: The system has a dual-redundant network. Each node has a duplicate, and can work independently if their duplicate is disconnected.

102: as 101, the system is dual-redundant in the sense any node has two independent network adapters, one for each network. Each network cable go to their distinct network switch to separate network A and network B. Network switches are installed at separate locations, as well as Control computers and Operator computers are divided through either bridge, cube or chairs, depending on the system. Each designated location can be damaged, without the communication between nodes disappear. Each node is also either connected to powers supply A or power supply B where either one power supply would be damaged, the remaining power supply would supply sufficient nodes to maintain communication. This is shown in appendix A, illustration 1 and 2.

103: Each network function independently as network A and network B is divided on each node in several ways. Each network is divided as each node has minimum two network interface cards (NIC). Each NIC have their own unique MAC address in addition, network A and network B is created with their own Subnet IP address. This gives network A only access to MAC addresses to NIC's connected specific to network A and network B only access to MAC addresses to NIC's connected specific to network B. This would imply if any package going from network A accidently ended up in network B, any network B node would send the package to the B switch. The switch would drop the package since its MAC address table

would not contain the receivers MAC address since this MAC address lies within network A, and in addition have no default gateway to send off unknown packages.

104: The system does not have a solution for this demand, and is therefore this demand will be taken into account to improve the system.

105: The system does not have any monitoring over the system other that all Operating computers can monitor their own network traffic over a standard Windows XP monitoring. This needs to be improved to have a total view over the networks traffic.

106: The network switches can be seen as the network controller for the current system. They will automatically resume to normal operation after a power failure. This is an ok thought, but what If the switch does a hard reset after a power failure?

107: The system uses the CC's to be synchronized. The OS's collects the CC's time to be synchronized.

108: The system and its components have already been tested for electromagnetic interference through other certifications. If there is other components added to the system for a solution, these will also need to be tested for this.

109: None of the systems is connected to any CCTV.

E. Malfunctions and restoration: 100 Failure effects

101: Definition of "part" is not set, but we conclude with part as node. Switch A can be shut down, and the system will still operate with switch B. Any other node are either redundant through 2 or more nodes with the same capability.

102: Depending on the system, the ICS's response towards malfunction today is varied. Considering MT's IBS system, there are no direct changes to the system if one node malfunctions. All nodes have a duplicate node for redundancy, which will take over if one node malfunctions.

103: Today there are measures where if the entire network falls down, there are stand-alone nodes who receives serial data from sensors to apply to such a demand. Making the

network protected enough, should make this fallback arrangement over redundant compared to safety and could possibly be removed.

F. Network test and verification

101: There is a need for a decent documentation for a test through the network to protect against different types of scenarios such as broadcast storm. There is mention about node individuality, but considering the wish to be fully flexible to have any information on any screen, node individuality is too much segregation compared to what is desired. Another important factor to make the system protective enough to make this demand over redundant.

Improvement needed

By looking over the demands from DNV GL, there is a need for improvement and change in the system. The system needs monitoring of the network and it needs a better protection towards broadcast storm. As many of the products need certification for use offshore, there is a desire to use the current products to recreate the systems towards these demands.

5. Suggested solutions

To make the different systems certified towards DNV GL regulations, all of the demands either needs fulfilled or made over redundant.

5.1 Self-protective nodes

```
if (buffer_next[33]==0xff)
{
MSS_MAC_prepare_rx_descriptor();
dc++;
}
```

Figure 10: An IF sentence, checking for broadcast messages

Every node should have their own protection towards broadcast storm or other errors the might occur on the system. There has already done a few of these measures already after examining some of the products. In both the IOB leaver cards and the IO cards there is hardcoded a protection against broadcast messages. Giving a hardcoded protection against broadcast storms. This protection starts at layer 2, as this programming denies any packages from *.*.*.255 (0xff) as shown in figure 10. All other nodes do not have this protection against broadcast messages, and therefore must handle all broadcast messages and use more CPU power.

5.2 Adding monitoring nodes

Create an additional computer to the network that monitors all networks. This computer will monitor both networks with the monitor software to monitor the network and to send out commands to the switches for broadcast storm filtering. This will also be used to send an alert to the system to say if any rules are broken. This computer will also have the

configuration to the switches and have a small software checking if the configurations are in order. If not, the software will update and restart the switch.

The issue with this solution is to add another node to the system, which also needs monitoring. To make the system able to be fully functional with a single point of failure, two additional nodes are needed.

5.3 Self-sufficient Switches

A managed switch is able to monitor its own traffic and close necessary ports through its configuration. By using the existing switch, it has configuration to protect each port against any broadcast or multicast storm with a broadcast limit. If this limit is exceeded it will shut down the port. Effective and precise solution to protect against any flooding of the network.

5.4 Anti-virus

The system today, do not have any sufficient security for viruses. As the system connects to unknown amount of USB devices through their testing and maintenance, there should be an up to date virus scan on the system. Even though the system is locked to the internet, it will still be connected to the internet at some time, virus may also affect the system through these USB devices. The system can be scanned by the project engineer, as part of the maintenance. As some systems runs smoothly over a long period of time, and the control checking of having an updated anti-virus database carried with the project engineer at all times, it is not seen as an optimal solution. Another solution could be to have an anti-virus software on the VRAG computer which is continually online, to be up to date at any time, and could scan the system every time the VRAG was in direct contact with the system. Depending on the level of maintenance, there could also be a demand for the ship's crew to activate the connection for this purpose alone.

5.5 Evaluation

Suggestion one is not possible to achieve. The hardcoding cannot be implemented on all nodes in the system considering the broadcast system is used to acknowledge different nodes to each other by using ARP. Even though each node would be possible to protect themselves towards a broadcast storm, the flooding of the storm would still fill up the network with unusable data, and the important data would not get through. Adding more nodes is also not a good solution. More nodes means more elements can go wrong, it also elevates the costs of each system. Using a monitoring software is something achievable and also a must considering the demands from DNV GL. In addition the checking of the static IP addresses on the switches is a good solution to check their configurations, but relying on switch configuration for protection is not a good solution as some configuration might be lost even though the IP address would stay the same. Self-sufficient switches would come under same advisement. If one switch configuration goes down, the system is then vulnerable to broadcast storms. Anti-Virus might seem redundant considering the system is a closed network. It still has connection to internet at some point, and during services, USB sticks connected to nodes inside the network.

6. Solution

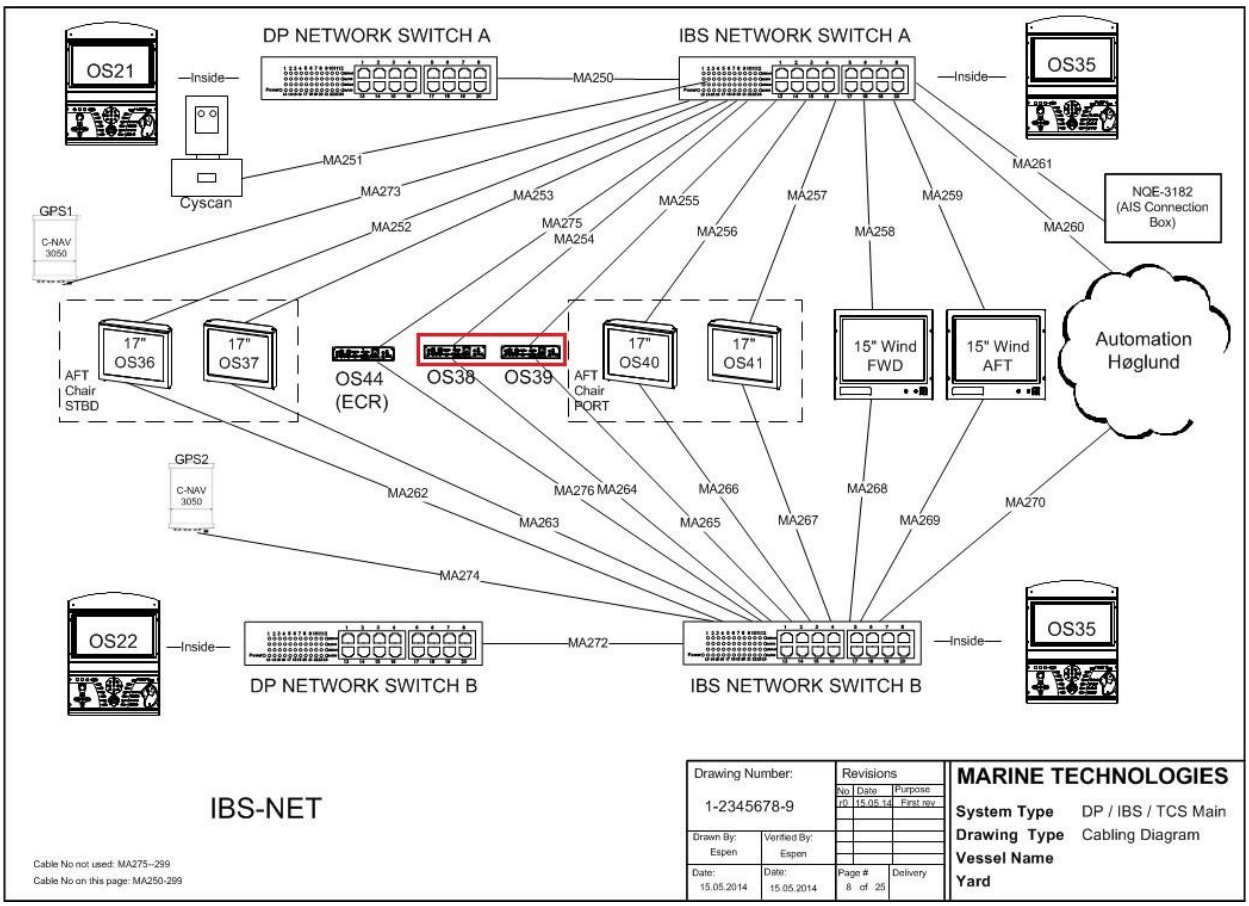


Figure 11: IBS System, with network monitor nodes marked in red

Adding additional nodes is not necessary to create a redundant protective net towards the existing systems. As any DP2, IBS or TCS contains 2 or more OC's, these can be used as the monitoring computers. Since the computers already today use different software to control the system through application manager, there should not be a problem to implement another software for monitoring and controlling the network. By either using an existing monitoring software or developing such a software, the network will be monitored and controlled. This software has several tasks it needs to uphold, such as monitoring the traffic, check switches for configuration loss, protect against broadcast storm and give any alarms necessary. Using an IBS as a base as seen in figure 11, the red computers will have the monitoring software implemented and will control and set alarms if a node malfunctions.

To protect against broadcast storms, the software will either itself control or will set off a command to make the switch turn off the actual port where the broadcast storm is coming from. With these improvements, the system would comply with all demands from DNV GL.

6.1 New technology

To comply with the DNV GL regulations there are several new technologies needed to the current systems. All these technologies are either already used in at a normal business network or on a larger scale network, either a big company or an Internet Service Provider (ISP). The reason these technologies is not in use on these systems today is that the focus has not been on the network itself, but on each element within the network. By adding several of these technologies together, there is a possibility to comply with all of the DNV GL regulations.

6.1.1 Network monitoring software

To comply with DNV GL standards, a network monitoring software is needed. For this thesis there has been chosen a software program between three different network monitor programs. Different software are available and by looking at Weathermap, Spiceworks and PRTG Network Monitor, the most professional and adaptable software for this task was PRTG Network Monitor. This monitoring software contains much information and data handling, it is not possible to create a prototype for this thesis given the limited timeframe.

The PRTG Network Monitor is created by Paessler. This company focuses on network monitoring solely and have created a good software which uses Simple Network Monitor Protocol (SNMP). Through this software we are able to not only look at network traffic, but also check computer health. Each node in the network with the abilities of SNMP can create several sensors. In our case, the computer nodes will have several sensors for monitoring CPU load, Network load, and hard disk space.

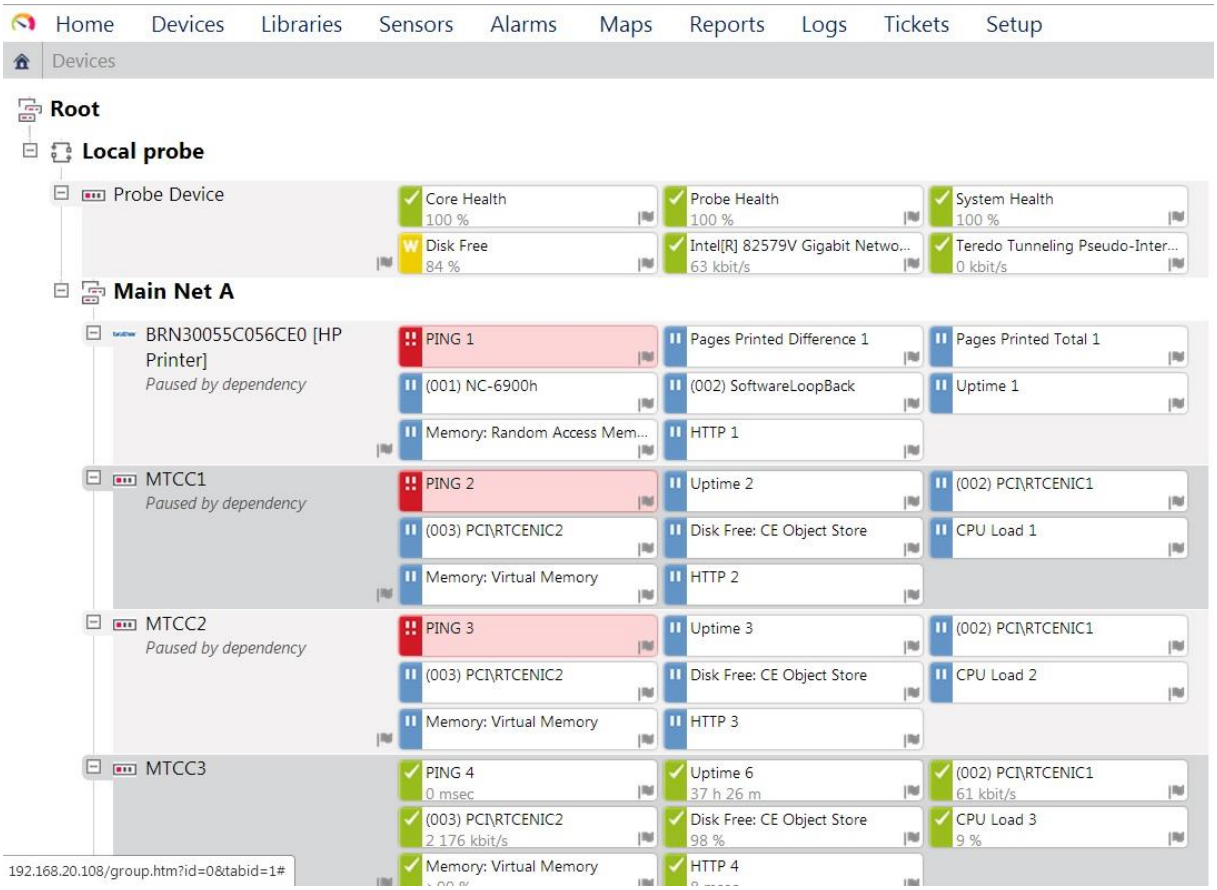


Figure 12: Illustration of PRTG Network Monitor Software

As you can see in figure 12 the software easily divides the sensors between the different nodes. One of the most important part in this system is the monitoring of network traffic. Not only does it monitor network traffic, it can also monitor the load of typical network packets such as TCP and UDP. Other tasks can be given to this system as it can monitor network errors and send out SNMP traps to almost any rules you set to the program. The idea is to use this software to monitor every active port on the switch and put a limitation trap of total traffic through the port. The system can expose any starting broadcast storm and take action towards the selective port. The goal is to send out a command to the switch to turn of the selective port and addition send out an alarm to the system, giving it an update on what is going on. Going through the software and communicating with the producers of the software, the software does not provide with a SNMP command to send to the switch, there need to be a third party included to give such a command.

6.1.2 Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) is used to manage or monitor different types of devices on a network. Different types of devices that supports SNMP is usually servers, routers, managed switches, printers and more. SNMP is what you could call a "middle-man" between devices you want to monitor and the management computer. There are three important elements in SNMP.

- Managed device
  - This device is the monitor for the network. All information collected from the agents are sent to this device and will be handled by a SNMP monitoring software. As mentioned the SNMP is a "middle-man" and needs an additional software on the managed device to read the information the SNMP collects.

- Agent
  - The agent is a small software that you have to install or is already installed on the different devices you want to control or monitor. These agents will send out information through SNMP to update the information collected from the Managed device.

- Trap
  - A trap is s a rule you set for an agent. These traps can be many different rules for a device. In a network view, it would be a good way to set a rule not to have a full buffer. If the rule is broken, the agent will send an alert to the managed device.

As the SNMP is a protocol to collect or change data on a node, this data is organized in a Management Information Base (MIB). MIB is a "catalog" structure for all the data. Each data-element where you can collect or change the information is called an Object Identifier (OID). The OID contains a unique number for each element [12].

A SNMP message contains different values of information. A suggested SNMP message could be:

Snmpget –v1 –c private 192.168.0.240 IfAdminstatus

This command will show the status of all ports in a node, such as a switch. The "IfAdminstatus" OID is to either get or set a status of a port to 1(up), 2(down), or 3(testing). The IP address given in the command is the hostname of the node. –c private is the community string with will allow you to access the information. The node can have several community strings for different type of permissions, such as read, and read/write.

6.1.3 Network Setup

For the current system which is used for the testing, the best available system is a DP2 system with TCS. In this system there are in total 4 switches, 2 for each network. In this test, only the main A and B network will be in use.

Nodes in the network:

- 8 Operation computers
- 3 Control Computers to DP
- 3 Control Computers to TCS
- 4 IO cards
- 1 Compact OS
- 3 Double thruster handles
    - 4 IOB leaver cards for each double thruster handle
- 6 Single thruster handles
    - 2 IOB leaver cards for each single thruster handle
- 1 Wheel thruster handle
    - 2 IOB leaver cards for the wheel thruster handle
- 1 VRAG computer
- 2 Mode selector units
- 4 Netgear Switches

Since this system is an actual product for a ship, the monitoring software will be used on an additional computer set aside from the original system. It will still be connected through the network, but to protect the product as it will go through configuration and a Factory Acceptance Test (FAT) it is best to keep the product as genuine as possible for the testing.

This computer will alone monitor the network and send out any commands necessary to the switches if any broadcast storm arises. This computer is connected to both main networks A and B, and will monitor both networks at the same time. In the PRTG Network Monitor software, we create 2 groups which will be monitored, one for network A and one for network B. Since A network is under the IP range: 192.168.0.* and B is under IP range: 192.168.1.* it is easy to scan the different networks to access the different nodes in each network.

The wanted result is a complete list of all of the nodes with SNMP capability and having several sensors on each node for network and other information.

6.1.4 Testing

The testing has gone under several stages since the system takes a long time to be created. As almost all components are created uniquely for each system, it takes time to create all the components. This is the first system with the new Netgear switches and therefore the choice of system for the thesis. Time is also a factor when it comes to deadlines of delivery. As soon as this system is running with the correct configuration, it will undergo a Factory Acceptance Test (FAT) with a DNV GL representative present before it is shipped off.

Stage 1.

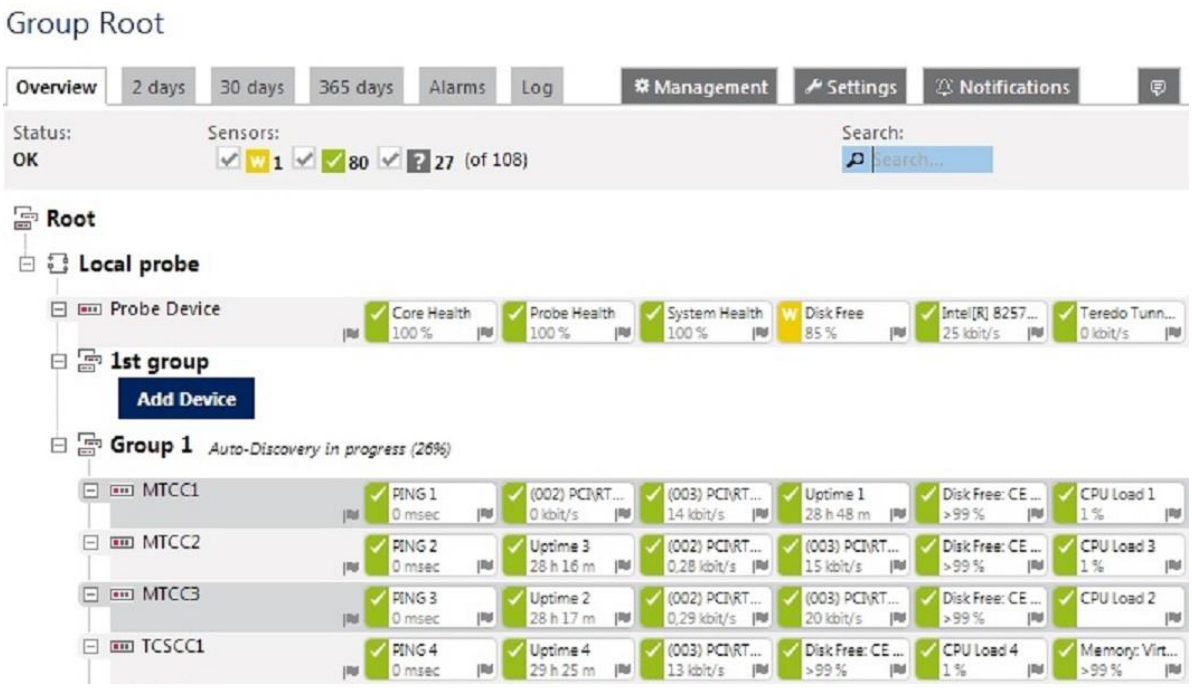


Figure 13: Scanning for nodes and sensors

The first test with the PRTG Network Monitor software, is to see how it handles and which nodes are connected or not. All of the CC, OC and switches are present after a scan through the network. At this stage, the thruster handles and the mode units are not in place. Since the IO cards use FPGA software, SNMP is not included and these cards deny any Ping request. The only connection in the software where we can see they exist is through the ports on the switch. The switch automatically creates a sensor for each active port when scanned. On each node, we can see several sensors, and can include any number of sensors, depending of the configuration of the node. Whenever a sensor is created, an e-mail is sent to the administrator, giving the administrator update on every single change in the program. It is possible to study each sensor in detail. On these sensors, we can watch a live feed of traffic through the SNMP data sent back to the monitor computer.

Each node has its own settings and notification. These notifications are the importance of protection for this thesis. To set notifications gives many possibilities towards the monitoring of the network.

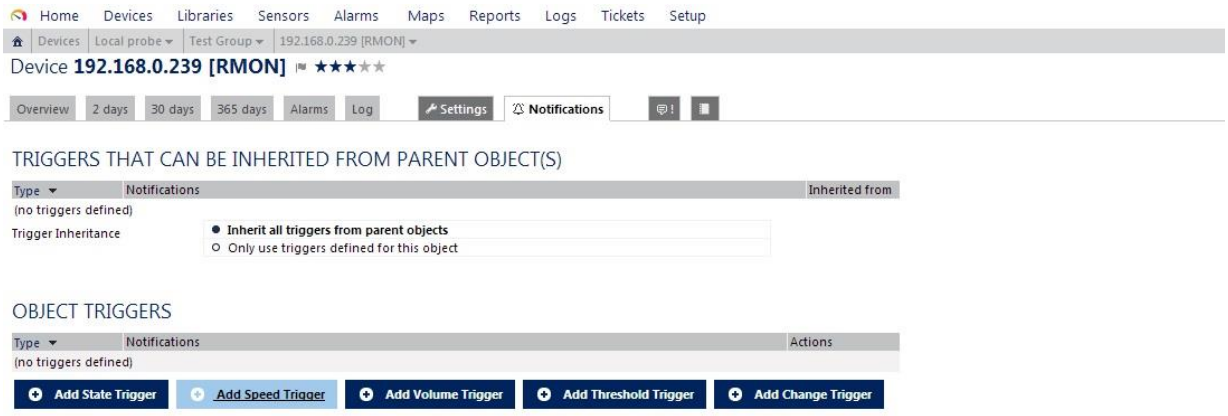


Figure 14: Notification or trigger (trap)

Notifications are the SNMP traps and can activate several types of alarms. The automatic standard is an e-mail. As seen in Figure 14, there are different types of trap settings. It is also possible to build up the network in a tree topology as seen in figure 13. This could be very helpful if different traps are set through different networks as a notification can be inherited by parent object.

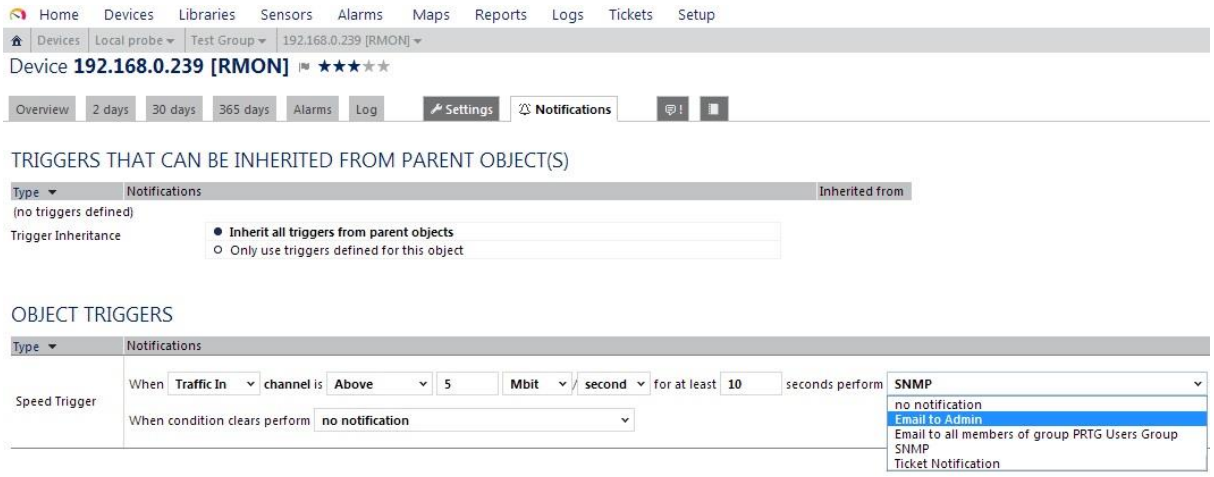


Figure 15: Setting a speed trap

Looking on how to set a speed trap, which is our focus, we can decide on many different values. Figure 15 gives a good view on what different options is given. By setting a trap of received traffic in a short period, an e-mail is sent immediately after the traffic exceeds the trap setting. This gives us the confirmation that the trap settings work.

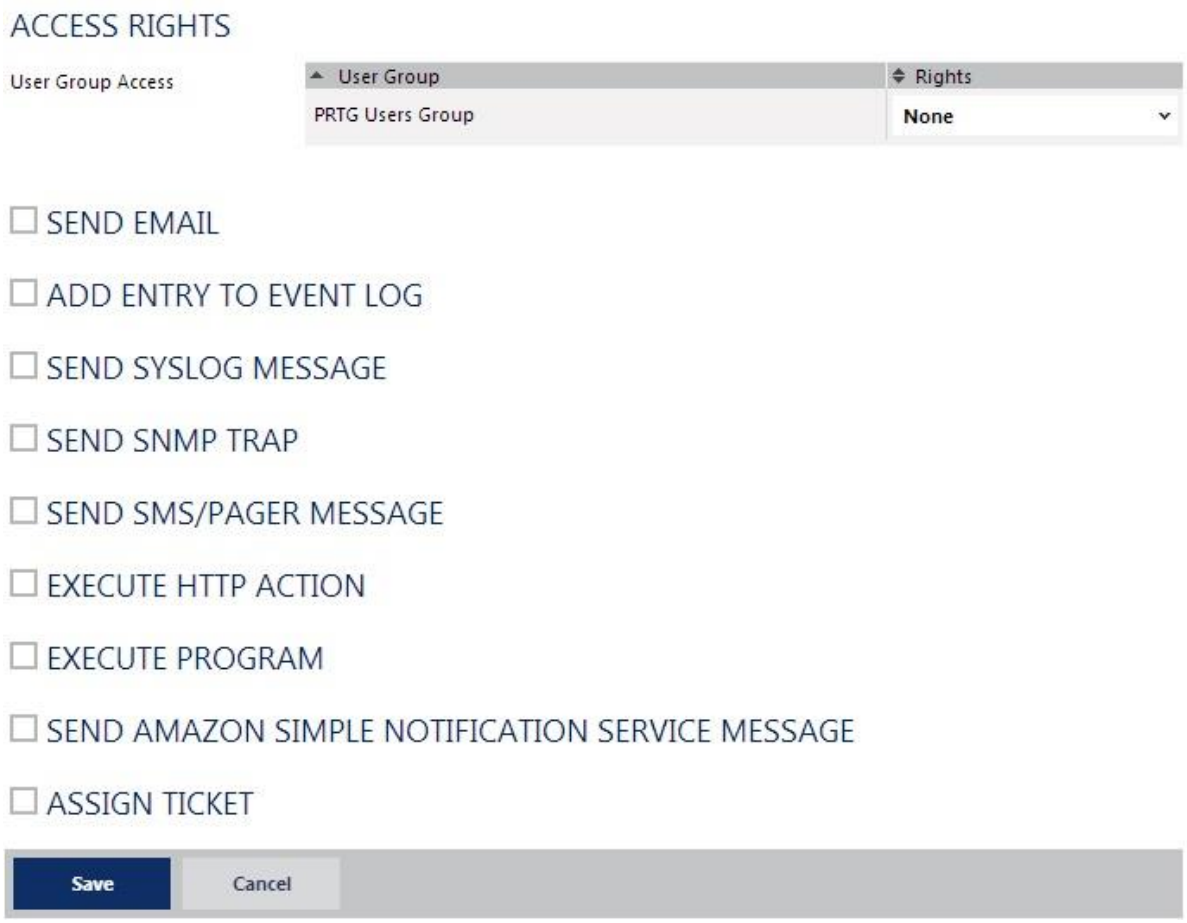


Figure 16: Adding new type of notification

Accessing more advanced settings on this software, we see the possibilities to trigger an execute program if a trap is triggered as seen in figure 16. Either by using this execute, or send a SNMP trap to a third party software, to shut down the broadcasting port.

Stage 2:

In the second stage of testing, a small program runs a broadcast storm from OS1. The system is rescanned, since all nodes are in place. The IOB Leaver cards responds on ping, but not on SNMP requests. This time the focus is on one network and see the reaction of PRTG Network Monitor when a broadcast storm is active.

A small program sends out 4000 packets continuously with a 60-byte size. The broadcast is a 255.255.255.255 broadcast. This means all nodes needs to receive and interpret the package before throwing it away. Both IO and IOB leaver cards have a hardware blockage on broadcast messages as they never need to receive any. The switch settings are set to 5% of

broadcast storm threshold. Since different network adapters are connected to the switch, this will just allow 5% of total capacity of each node. A 100 Mbit node will only have 5 Mbit capability through the switch.

The first noticeable experience is the CC's. Both TCSCC and DPCC get warning signals of high CPU usage before some of them disconnect. None of the other computers seems to have any bigger effect from the broadcast storm in the early stages of the broadcast storm.

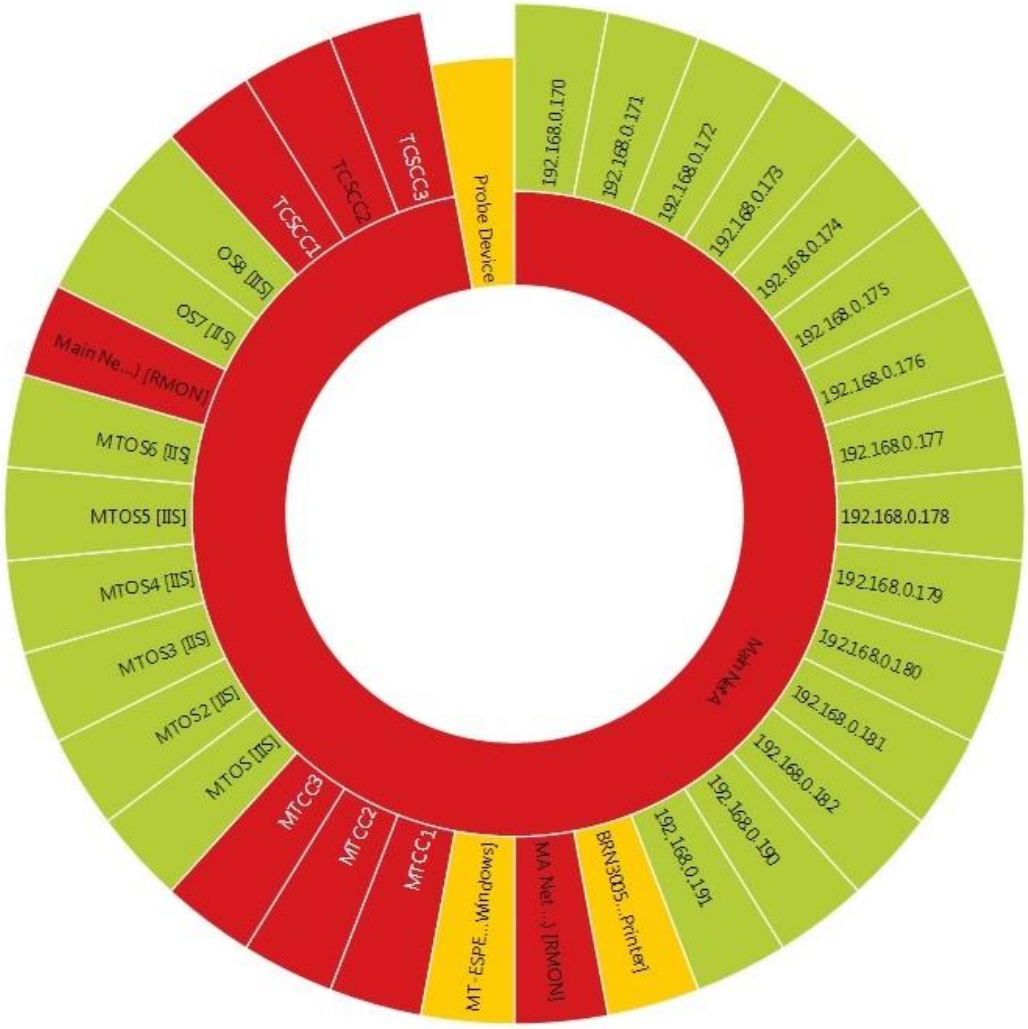


Figure 17: PRTG Illustration picture under the beginning of the broadcast storm. Red: Alarm, Green: On, Yellow: Warning

The next noticeable and unexpected, the switches ping reply to PRTG software stops responding. Entering the switch sensors, all other sensors monitoring the ports are set on pause, since the system no longer have contact with the switch. Even though the switches does not reply to ping, as figure 17 shows, the other nodes are still active and sends out SNMP messages. On the MTOS software on the OS1, the monitor confirms the CC's high level of CPU load as PRTG software. The CC computers start to stabilize after one or two restarts. They are able to send SNMP information even though their CPU load is between 90-100%. Reading off the network monitoring on the broadcast computer, it only uses up to 3% of its capability. Since this is a 1Gbps capable network adapter, this implies that the switches and CC's have problems with a broadcast storm of 30Mbps. All of these nodes have 1Gbps network adapters.

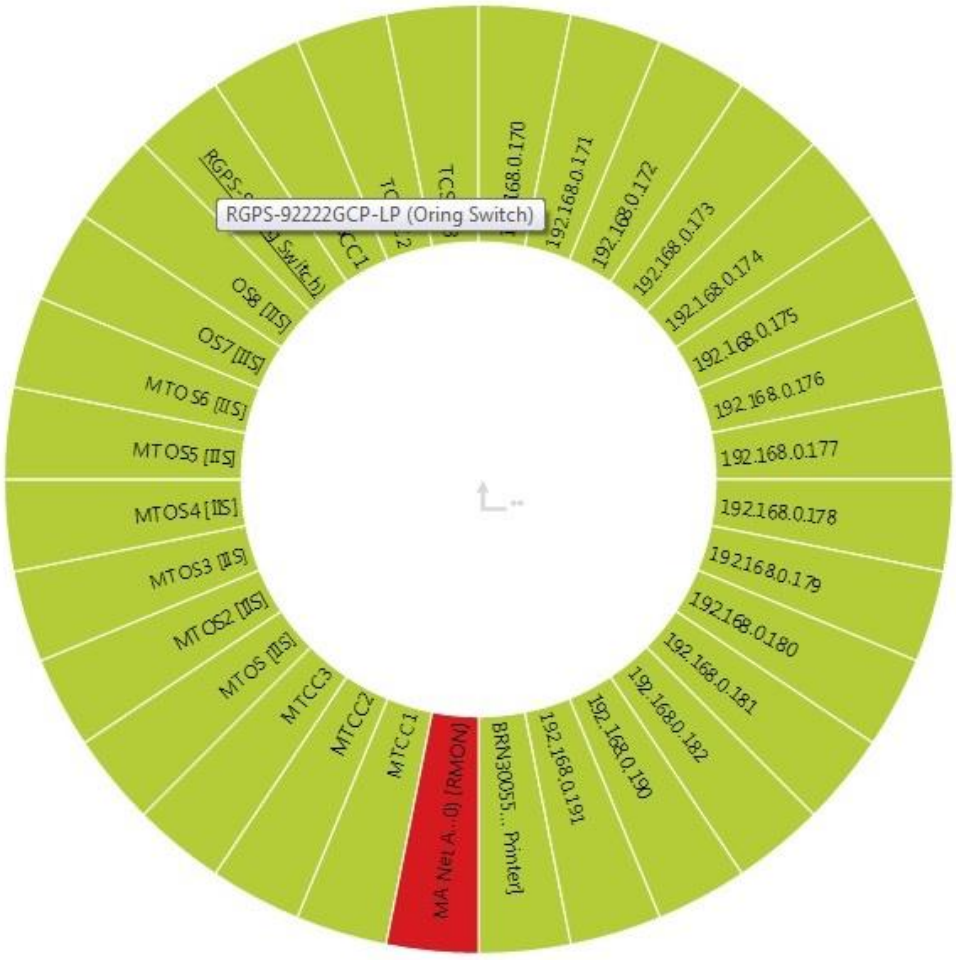


Figure 18: By exchanging a switch, the system operates more fluently during a broadcast storm

A concern arises since the switches are not capable of replying to ping or accessed through HTTP so soon in a broadcast storm. By using another available switch, an O-ring RGPS-92222GCP-LP, it is possible to test if this is an issue with all types of switches. Replacing the Netgear switch and configure the O-ring with the same IP address, the system is up and running with no issues.

The expected results starts again with the CC computers starting to fail and restart. The other Netgear switch also loses its ping capability, and so does the O-ring. After a minute of broadcast storm, the O-ring switch returns ping reply, and have no problems with the broadcast storm as shown in figure 18. It is even able to be accesses through HTTP, and have no problem accessing the entire web interface.

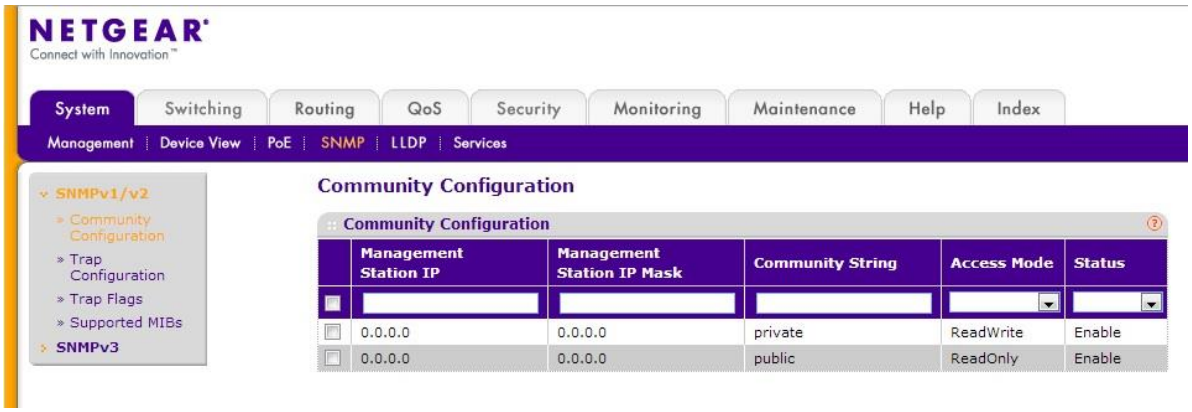


Figure 19: Netgear web interface

The second Netgear switch is also able to show its web interface, although with a very long delays. On the O-ring switch, it is easy to access the port configuration, shut down the port connecting OS1, which turns off the broadcast storm from the rest of the network.

During both tests, it was also noticeable that one OC and one IOB card lost their ping once or twice during the broadcast storm.

Step 3.

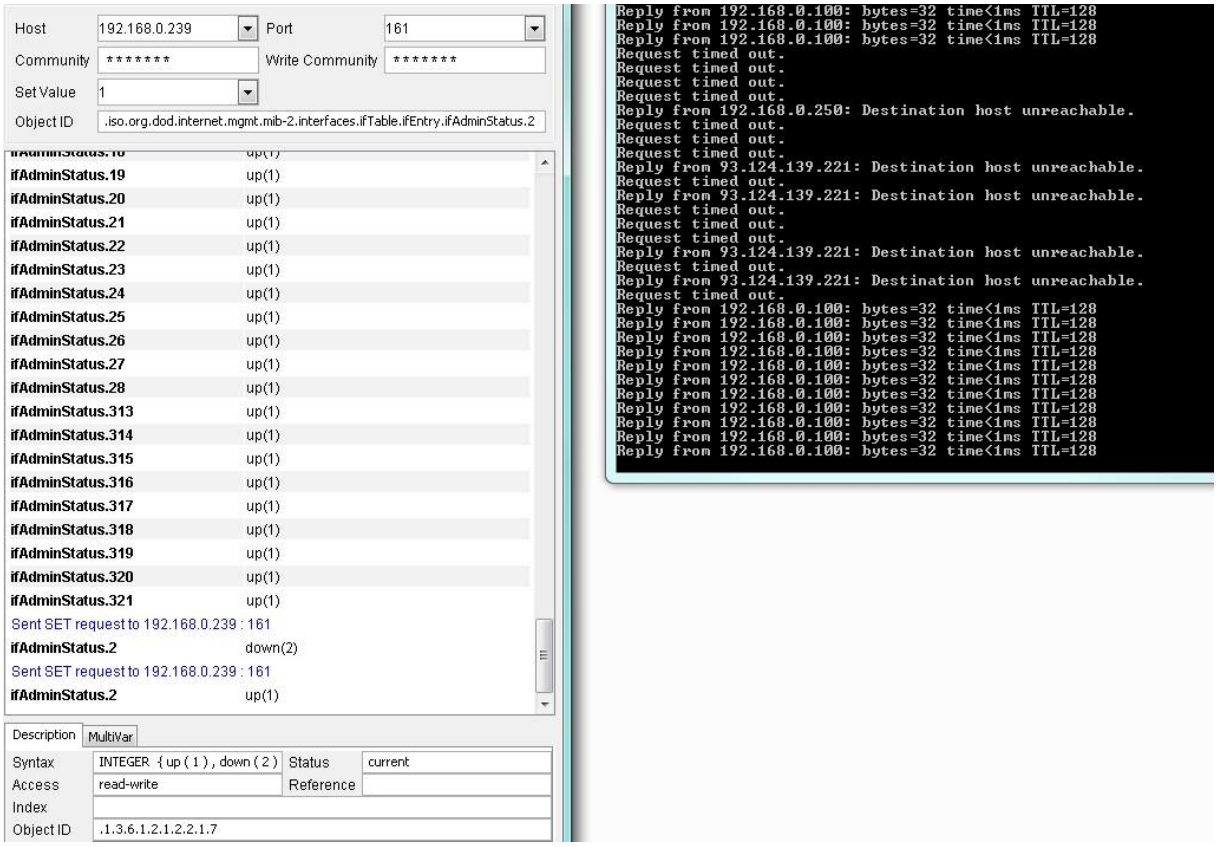


Figure 20: Turning on and off the switches port while doing a ping request to another computer

To protect against this broadcast storm it is desirable to be able to close the specific port receiving the broadcast storm. This can be done by sending an SNMP command to close the designated port. Using a MIB Browser program the selective OID to turn off a port is available to send to the switch. The OID used is ifAdminStatus. In figure 20, it shows the status of the ports after a SNMP get request. While sending a continues ping request to another node through the switch (192.168.0.100), there is a sudden stop of response after a SNMP set command to shut down the port this computer resides in. Even during a broadcast storm, this command is still going through both type of switches.

6.1.5 Test Results

From the results of the test, it is easy to notice the fragile CC. Considering the CPU load were considerably high during a broadcast storm compared to another node such as other OS. These computers had a CPU load of less than 50%. An OC is manufactured with higher CPU considering their task are more demanding than a CC, but the CC do have a good CPU for its usage, and it is not a single core CPU. A dual core CPU should handle the broadcast better, and after a small discussion with the developers at MT, they assume the windows 7 CE image they have created for the CC, does not include the usage of two cores. The reason the IOB cards did not crash during the broadcast storm is of its hardware protection against broadcast. The package stops early in the handling process and therefore the broadcast storm do not generate high CPU load. The MTOS software did neither set off any alarm mentioning the loss of connection to the IO cards, determining the broadcast protection on these cards as well.

The switches response is also a concern. Considering it is not able to reply a ping request or be able to access its web interface, determines its focus only on transmitting the packages through the network. Even though the command got through the switch, this is still a concern.

The test shows a solution to make the network fail-safe towards single-point failures can be done with including monitoring software and using SNMP commands. One can say the network today is protected against single-point failures, as it is redundant on every node. This is not completely true if a broadcast storm appears on both networks it will flood switches on both sides, and it is no longer a single-point failure. With the protection given through the test, there will be protection against any single-point failures at any network.

6.2 Other Improvements

Even though the test results shows a good solution to protect the network against broadcast storm, and is a possible solution to get the system certified, there are still things which can optimize the network and its traffic.

6.2.1 Multicast vs unicast

Most of the traffic used in the system is unicast traffic. The reason for this is in MT's early stages they only had 2-3 nodes on their DP system and the nodes could easly process the unicast messages for each node. As the systems have grown into IBS and TCS there are many more computers requiring these packages. Considering the growth of these systems, unicast messages would put more CPU load on the transmitting nodes. Multicast messages would simplify the CPU load on the transmitting nodes and on the switch. The issue with Multicast messages is the need of IGMP Snooping to work.

6.2.1.1 IGMP

IGMP is a communication protocol, used for establishing multicast group memberships. In multicast, it is needed for the switch to create a group of memberships to duplicate and spread out the multicast message to the right nodes. IGMP is often used in video streaming to lighten the load of the source. The source node does not have to duplicate a package for every node watching the video stream, but send out one stream to a switch or router, where the switch will duplicate the package and send it to its respective recipients [13].

6.2.1.2 IGMP Snooping

IGMP snooping works in layer 2. IGMP snooping works the same way as IGMP, but it works with MAC addresses. If a multicast message is sent to a switch without IGMP/IGMP snooping, the switch will have no group to list who of its ports needs this information, so it will handle this multicast as a broadcast [13].

6.2.1.3 IGMP Issues

IGMP exists in different versions and this create an issue with IGMP Snooping. If the nodes contain different versions of IGMP such as version 1 and version 2 the multicast messages would actually not be received at all the recipients. IGMP version 3 has been on for many years and is backwards compatible with both version 1 and version 2 which would solve this issue. Norsk Elektronisk Kommisjon (NEK) has done research and tests towards IGMP and IGMP Snooping and concluded that IGMP Snooping is not allowed in IEC Standard 61162-450 (450-standard). This standard is towards ship communication and DNV uses this standard towards their demands on MT's network. Having contact with NEK representative about this issue, he explains the problem exist in equipment made without complete IGMP abilities, creating the conclusion of denying IGMP Snooping in their standard [14]. He does mention that the 450-standard is not demanded in a ship bridge from their view, but it depends on other certification companies.

> *«To get approved for a 61162-450 network, the standard needs to be followed for what is defined as a network. 450 will neither allow direct connection to other networks through switches, routers or other similar equipment. On the other hand, your solution could be approved for usage such as a ships bridge if the class (meaning flag state) approves the solution as good enough for its use. Therefore, you do not need to use the 450-solution on all the ships network. »(translated)*
>
> *Ørnulf Jan Rødseth.*

In addition there is a new ongoing standard which is not finished, where they are evaluating the demand of having all equipment desiring the 460-standard to have full IGMP support. This will conclude in future standards IGMP could be demanded and therefore IGMP Snooping would the supported by the certification companies.

6.2.1.4 Alternate IGMP solution

Depending on DNV GL's decision, there is an alternative to solve the IGMP Snooping solution towards third party equipment. Since the system created at MT is a closed network with only their own products connected to the system, this network could have IGMP Snooping on the inside of this network. For the third party equipment, it would be possible to create a third network, network C especially for third party equipment to be connected to the specific nodes they need to communicate with. This third network will then be set without IGMP Snooping and be under the 450-standard.

6.2.2 Quality of Service

Netgear GS728TP switch is a new product in MT's systems and have more possibilities than the old one. One of the big improvements is the increase of QoS queues. Often a switch today has only 2 QoS buffers, meaning it can make traffic either important or not important. This new switch has the possibilities to manage traffic into several queues, making it easier to focus on which type of traffic is important. Netgear switch also contains a storm control, where you can set a broadcast and/or multicast limit to protect against a broadcast storm. Considering this storm control does not take into account the type of traffic, the netgear support has given the confirmation that QoS is handled before the switches storm control. If the storm control is used, it would be preferred to mark important data going through first, to make the unimportant data be cut incase of high traffic being cut off by the storm control.

"Regarding your inquiry, QoS is being handled first before Storm Control.

Regards,

Anna Bagasan
Level 2 Technical Support
NETGEAR, Inc.
http://support.netgear.com"

Quality of Service (QoS) is a protocol used in almost any larger network to control traffic. What QoS actually does, is after the switch has received its packages, it looks at the header to see what package it is and puts it either in a higher level buffer or a lower level buffer. As the Netgear switch has up to 4 buffer queues it is easier to divide different types of traffic into groups to be certain specific traffic is prioritized.

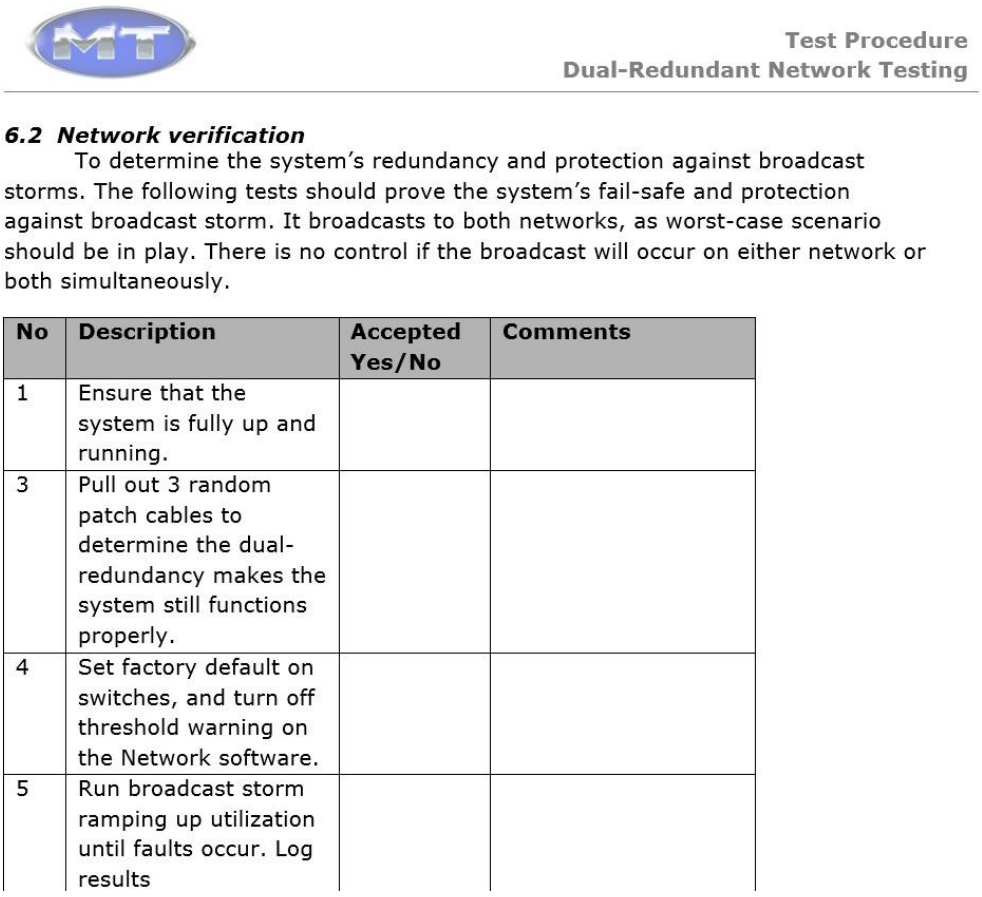
6.2.3 Affinity

Affinity is a way to divide CPU cores to different types of workload. The idea with this is to divide workload more controllable. If one application demands high CPU load, it will not set another application at pause since it is appointed another CPU core. With this kind of segregation there is a possibility to protect CPU load towards malfunctioned software. Affinity has the possibility to assign different core's of the CPU to different NIC's. [15] Going through the different layers in the OSI-model, no matter how high you segregate, at MT's systems you cannot divide the application layer, and therefore is affinity not a complete segregation. Besides, putting different software on different network will only remove redundancy.

6.2.4 Fiber cable between switches

As these managed switches are able to use fiber cable on a few of the ports, this could assist the network of preventing a bottleneck between the switches. An optical fiber cable is a cable made of glass instead of copper. These cables uses light to transmit data, and can therefore send data at a much higher speed [16]. Today, there are no issues with bottleneck traffic. The project engineers even divide the heavy load traffic such as radar computers, into one single switch to prevent a bottleneck. This is a good solution for now, but making a simpler connection preventing limitation of radar computer placement, an optical fiber cable between switches should relieve the system for any bottlenecks between switches.

6.3 DNV GL documentation



Test Procedure
Dual-Redundant Network Testing

6.2 Network verification

To determine the system's redundancy and protection against broadcast storms. The following tests should prove the system's fail-safe and protection against broadcast storm. It broadcasts to both networks, as worst-case scenario should be in play. There is no control if the broadcast will occur on either network or both simultaneously.

No	Description	Accepted Yes/No	Comments
1	Ensure that the system is fully up and running.		
3	Pull out 3 random patch cables to determine the dual-redundancy makes the system still functions properly.		
4	Set factory default on switches, and turn off threshold warning on the Network software.		
5	Run broadcast storm ramping up utilization until faults occur. Log results		

Figure 21: A part of the test document in Appendix A

Parts of the thesis is to create an argumentation to DNV GL to show what should be needed and what MT should do to create a good, fail-safe network. Using picked up information and how a solution could be, a test document is created to give DNV GL a suggested test procedure on how a network can be fail-safe compared to their demands. In this test document, there is a simple explanation on how MT's network works, and what measurements is taken to protect the network against different malfunctions. Through the document, there are tests towards dual-redundancy, and broadcast storm. Considering worst-case scenario, the test demands 3 random patch cables to be disconnected, and a broadcast storm occur after this event. The system should alarm for all 3 cables to be disconnected, and show off an alarm of a possible broadcast storm, and provide an alarm of why the selected node is disconnected from the entire network.

6.4 Discussion

Their systems are protected to a certain degree against broadcast storms as a worst-case scenario. DNV GL, use this incident as the biggest issue they see with a network. Their protection do not stop the broadcast, it just limits the flooding, and no element is checking if this protection is actually active. Adding monitoring software such as PRTG Network Monitoring Software, to nodes will get their system closer to the demands given. This software gives a good view of different sensors available at each node, it could be a good solution to monitor more than just network traffic. Sadly, it does not provide the perfect ability to send a simple SNMP command to the switch to turn off the threat of a broadcast storm. This is a negative blow for such a good network monitoring program. If this program is used, there is needed an additional software to deliver this command for the thesis's solution to be completed. Considering the type of alarms and commands able to be sent from PRTG, this software is needed to be created. Developers at MT have long experience with both C-sharp and C++ programming, and they have the necessary knowledge to create such a software. Putting time aside to create a small program like this, and in addition, use time to implement PRTG Network Monitoring software to their current application manager could be the simplest way to implement network monitoring and protecting. Creating their own monitoring software might be a longer road, but a more efficient and optimized towards their own systems, especially considering alarms as their system have an advanced alarm system where every node checks each other. Creating their own software will take longer time, and the costs would be considerably higher to make a good implementation.

7. Conclusion

From the current version of the system, it needs a network monitoring system. The best suggestion would to develop a software for network monitoring purposes. As one of the demands from DNV GL's, there is a need for monitoring of the network although they do not describe how detailed the monitoring needs to be. Creating a software will be the best opportunity to monitoring more than just the network. With the SNMP technology, much information given to MTOS can be put through this software as the hardware and network maintenance, making each software more focused on its own task. The nodes do need to have SNMP activated to monitor more than just a ping reply. Each type of software on the nodes needs to be configured to support SNMP and what type of OID's can be collected from them. For the monitoring of the network traffic alone, this is not necessary for each node since the switch provides sensors to all the active ports. With their own software, they can easily implement the SNMP command to shut down a port. The possibilities are many to create this protection dynamically. It would also be easier to create the alarms and necessary adjustments to make the network monitor software communicate with the rest of the other software. As long as such an implementation is in place, there should not be any need for further protection from broadcast storms. Protecting the configuration on the switches are therefore unnecessary if the software is given these premises. As mentioned, the VRAG computer should hold an anti-virus software to scan the network each time the system connects to this computer. During maintenance of a system, there is no certainty the USB memory stick the project engineer uses, is virus free. Therefore, the project engineer should always set this stick on the remote access computer and access all the data needed through the network from this node, so the remote access computer can scan the selected stick before the connection between the stick and the internal network is connected. As the solution for IGMP is not set yet, it is an ongoing discussion with DNV GL and MT to make this approved for optimizing the network. With this thesis, it should provide enough documentation for MT to prove for DNV GL, that the 450-standard is not needed for a bridge network to give a fail-safe solution. As each system is different, there are different solution given. DP systems should change their switches into managed switches to be able to stop a broadcast storm through the developed software. IBS systems and TCS systems should only need to add this software to two or more computers to create redundancy against single-point failures. Another important factor is the

switches are set in a star topology. The recommended topology would be a ring topology. If a switch should malfunction, the main network would still be able to operate most equipment shared between other two switches. The documentation in appendix A is to give DNV GL a suggested solution on how to prove that a network is fail-safe. This document shows a solution on how to test this thesis's solution towards a fail-safe network.

8. References

[1] Yixin Zhao, Feng Lio.

The implementation of a dual-redundant control system *Control Engineering Practice, Volume 12, Issue 4, April 2004, Pages 445-453*

[2] Minh Huynh, Stuart Goose, Prasant Mohapatra

Resilience technologies in Ethernet *Computer Networks, Volume 54, Issue 1, 15 January 2010, Pages 57-78*

[3] Clarke, R. J.

Research Models and Methodologies
http://www.uow.edu.au/content/groups/public/@web/@commerce/documents/doc/uow012042.pdf [17.11.2013], 2005

[4] Snap Survey Ltd.

Qualitative vs Quantitative Research
http://www.snapsurveys.com/qualitative-quantitative-research/ [01.12.2013], 24.01.2013

[5] Kish, Paul

Category 6 Cabling Questions and Answers
http://www.belden.com/docs/upload/what_is_category_6_q-a.pdf [14.05.2014], July.2002

[6] Webopedia

What is the difference between IPv6 and IPv4?

http://www.webopedia.com/DidYouKnow/Internet/ipv6_ipv4_difference.html

[14.05.2014], January.2014

[7] wikipedia

Bit numbering

http://en.wikipedia.org/wiki/Bit_numbering [14.05.2014], January.2014

[8] Craft, Nix

Key differences between tcp and udp protocols

http://www.cyberciti.biz/faq/key-differences-between-tcp-and-udp-protocols/

[12.05.2014], May.2007

[9] Fairhurst, Gorry

http://www.erg.abdn.ac.uk/~gorry/course/intro-pages/uni-b-mcast.html

[15.05.2014], 10.3.2009

[10] International Elecrotechnical Comission

www.iec.ch [10.05.2014], 2014

[11] Det Norske Veritas

Nautical Safety

http://exchange.dnv.com/publishing/downloadPDF.asp?url=http://exchange.dnv.com/publishing/rulesship/2014-01/ts608.pdf [14.04.2014], Januar.2014

[12] net-snmp.org

http://www.net-snmp.org [17.05.2014], February 2014

[13] M. Christensen, K. Kimball, F. Solensky

RFC4541 – Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches

http://tools.ietf.org/html/rfc4541 [03.05.2014], May 2006

[14] Rødseth Ø.J, Christensen. M.J, Lee. K

Design challenges and decisions for a new ship data network

Rødseth Ø.J., Christensen M.J.; Lee K. (2011). [12.05.2014], September 2011

[15] TMurgent Technologies

White Paper: Processor Affinity

http://www.tmurgent.com/WhitePapers/ProcessorAffinity.pdf [20.05.2013], November 2003

[16] ebay

Gigabit Ethernet cs. Optical Fiber Network Cables

http://www.ebay.com/gds/Gigabit-Ethernet-vs-Optical-Fiber-Network-Cables-/10000000177629223/g.html [20.05.2013], August 2013

9. Table of Figures

Appendix A

MARINE TECHNOLOGIES

Document title:

Test Procedure
Dual-Redundant Network Testing

Document description:

Test procedure for MT's Network in IBS, TCS and DP Systems.

1.0	05/12/2014	First issue	EL	TH	
Rev.	**Date** mm/dd/yyyy	**Reason for issue**	**Issued by**	**Checked by**	**Approved by**

Table of Content

Document History

Issue no	*Affected Para-graphs*	*Document History*	*Reason for Change*
1.0		First issue	

1. Preface

Document Version Control:

It is the reader's responsibility to ensure they have the latest version of this document. Questions should be directed to the owner of this document, or the project manager.

Document Owner:

The primary contact for questions regarding this document is:

Espen Løvø
Marine Technologies LLC
Espen.lovo@mtllc.us

Privacy Information:

This document may contain information of a sensitive nature. This information should not be given to persons other than those who are involved in the project or who will become involved during the lifecycle.

2. Introduction

This document is the test procedure document for MT Network for verifying that the network is fail-safe. By going through different tests through the document, the network will show it may be approved for standards such as IEC 61162-450, depending on the certificates.

*Notice this test may need update in near future, considering a new IEC 61162-460 is in development.

2.1 Testing Facility

The testing will be performed at the MT office in Egersund.

2.2 Product Scope

The equipment involved in the testing is:

IBS system/TCS system/DP system

Etc.

3. Resource Requirements

The test requires the following representatives to be present and acknowledging the document is of the latest version:

MT:

MT Representative –

DNV GL:

DNV GL Representative -

Test Dates:

_____ _____

Signature
DNV GL

Signature
MT Representative

4. Test Preparation: Procedures and Documentation

4.1 Test Environment Illustrations

Figure 1 is an example of a network that contains types of nodes on an MT network. Depending on the number of switches, they are set in a star topology. Figure 1 only shows Main net A and Main net B.

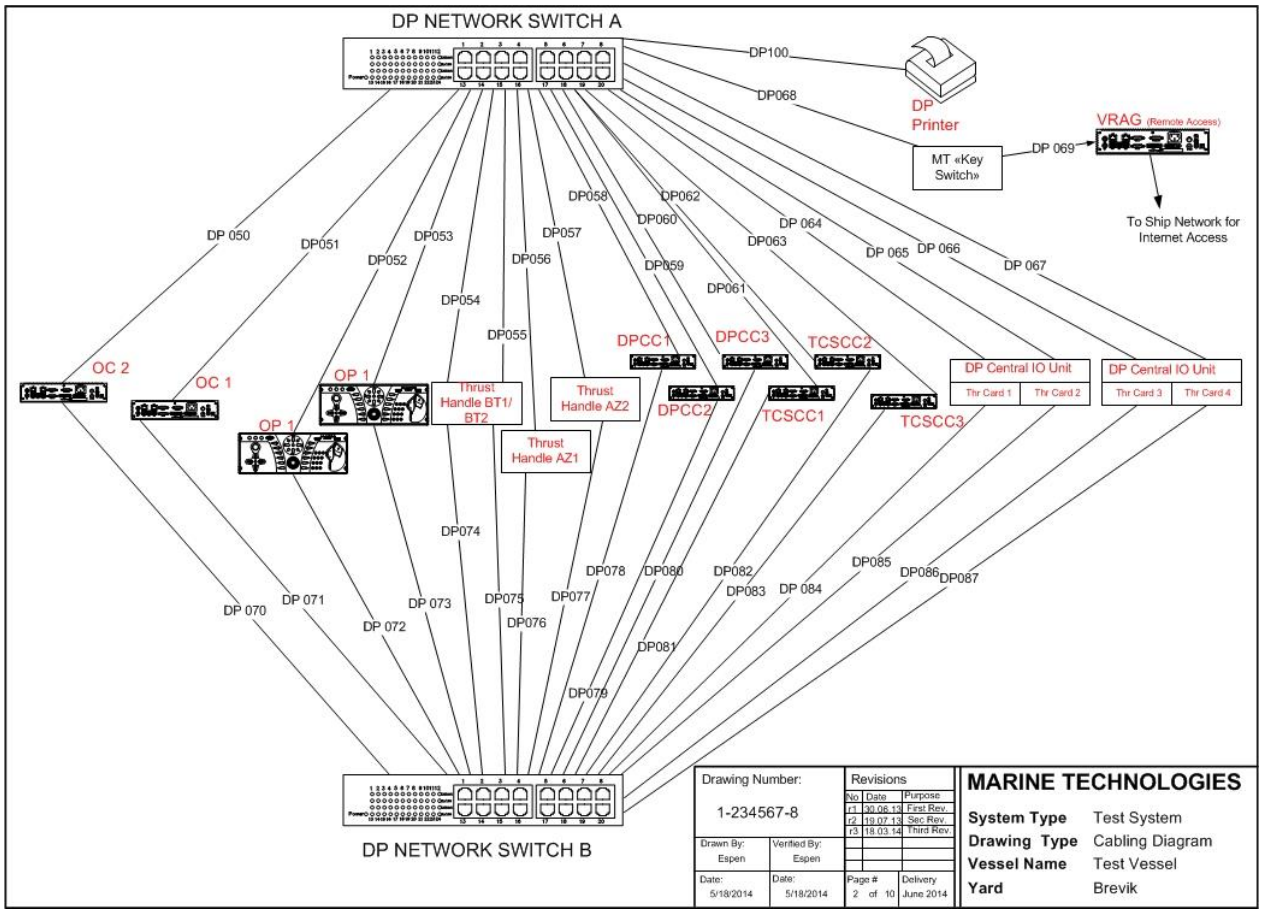


Figure 1: Illustration of network nodes and connections in a Main net A & net B.

Figure 2 and 3 illustrates the redundant network topology. For the navigational discipline, only the main system is relevant to consider. MFD stations on backup side is Independent Joystick, Backup Thruster Control and in some cases Backup DP.

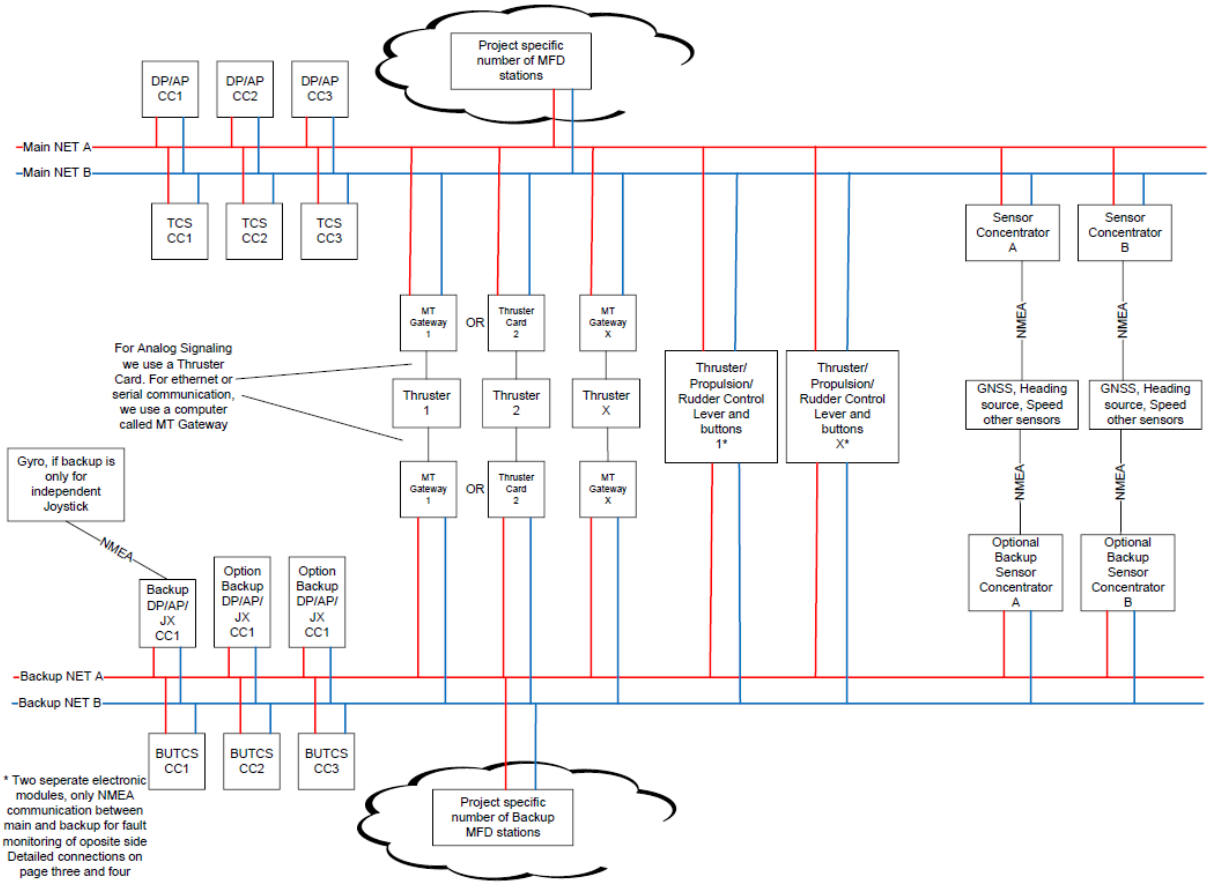


Figure 2

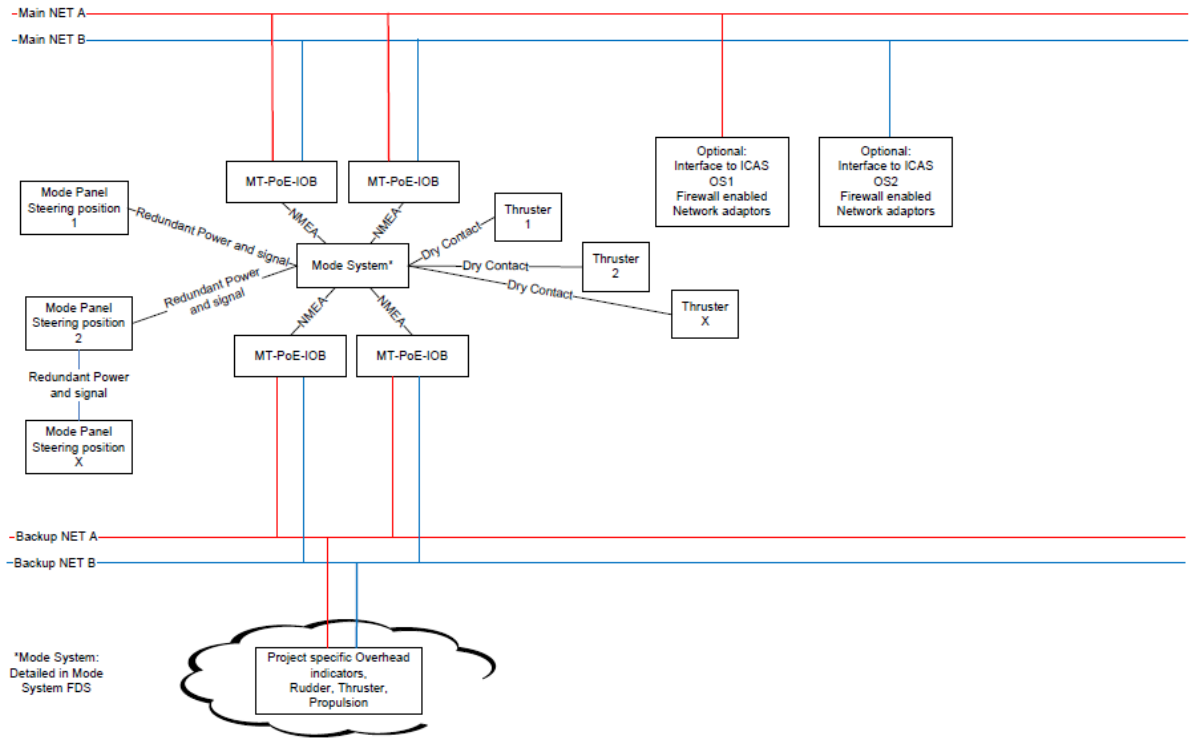


Figure 3: showing the connection to the Mode System.

5. Network Testing

The main system is a dual-redundant network, meaning it is protected towards single-point failures. Any 3 randomly selected network cables can be disconnected, and the system is still operational. In addition, there is a redundant backup network, completely segregated from the main network.

The Network monitor software is not set as slave or master in this system as they will behave independently of each other. The commands given by either will not destruct the commands of the other.

The DNV regulations will not consider the bridge system's networks as redundant unless documented and proved fail safe, hence will require sensors directly interfaced to Ecdis and Arpa in addition to network based sensors.

Quote DNV:

> *"An exemption from this general fall-back principle may be accepted for completely independent network systems including independent software. Approval may only be granted following documented design, failure analysis and testing verifying that any logical failure, including uncontrolled broadcast of data packets (network storm), of any computer connected to the networks cannot cause a meltdown of more than one of the networks."*

Marine Technologies topology uses two independent networks, no interconnection between them. Still all nodes has two network adaptors and it is known that uncontrolled broadcast due to serious software bugs, hardware failure (jabbering is not relevant in switched networks) or malicious software may occur. Broadcast is considered the one way to compromise both network by a single failure.

The network switches of type Netgear GS724TP and GS728TP that is in use in MT systems have the ability to turn of specific ports through commands sent by any connecting node.

MT do not use broadcast intentionally in they're systems. ARP requests are still broadcast and must be allowed to pass.

MT is configuring a broadcast threshold of 3% or 3Mbit/s. If this threshold is held for over 2 seconds, an alarm will be sent to both monitor computers, and they will individually send a command to shut down the designated port/s

The test will use a broadcast storm program to generate broadcast storms of various thresholds. The test will involve "unprotected" switches and the software turned off to determine the threshold of where the system starts lagging and eventually fails. It will then determine that when protective measures are implemented, the single node generating this will be compromised and alarms will be generated indicating loss of this node. The alarm should specify the command given to shut down the communication to the rest of the system.

6. Test procedures

The test procedure will only go through the main system.

6.1 System startup

The following tests will verify that the system boots up properly after a power outage and that all functions are available to the user.

No	Description	Accepted Yes/No	Comments
1	Boot up the system and check that all nodes are online		
2	Log-on to the Network Switch to determine its IP address and configuration is correct after		
3	Check the Network monitor software detects every node is connected to the switch		

6.2 Network verification

To determine the system's redundancy and protection against broadcast storms. The following tests should prove the system's fail-safe and protection against broadcast storm. It broadcasts to both networks, as worst-case scenario should be in play. There is no control if the broadcast will occur on either network or both simultaneously.

No	Description	Accepted Yes/No	Comments
1	Ensure that the system is fully up and running.		
3	Pull out 3 random patch cables to determine the dual-redundancy makes the system still functions properly.		
4	Set factory default on switches, and turn off threshold warning on the Network software.		
5	Run broadcast storm ramping up utilization until faults occur. Log results		
6	Configure switches back to MT default state, and turn on threshold warning.		
7	Repeat test 5 and confirm the protection sets in and the system is operational. No broadcast storm should be detected on either Network Monitor system.		

With this test, there is proof that the dual-redundancy makes the system still operational if a single-point failure occurs. In addition, prove that the system is capable of protecting itself against a broadcast storm created at a random element.

Since the system is capable of protecting against broadcast storms and single-point failures, there should not be any need for independent computers connected to independent sensors. As the network is fail-safe and protected against such errors as a broadcast storm.

The system uses IGMP Snooping to optimize the network, and to minimize the traffic. Since all nodes inside the system is either produced or handpicked by MT, all these nodes have full IGMP implementation, making IGMP Snooping compatible on the network. All future nodes connected to the network will be approved by MT, assuring any node connected in the future is IGMP compatible.

Approved and signed:

Date: _____ Original: ___

Copy: ___ Copy number: ___

_____ _____

DNV Stamped MT Stamped

_____ _____

DNV Representative MT Representative